Standard Technical Specifications Combustion Engineering Plants

Bases

This electronic text represents the Commission's current Standard Technical Specifications. This document is updated periodically to incorporate NRC approved generic changes to the Standard Technical Specifications.

The last Standard Technical Specification NUREGs were published as Revision 3 of NUREG-1430, NUREG-1431, NUREG-1432, NUREG-1433, and NUREG-1434 in June 2004.

B 3.2 POWER DISTRIBUTION LIMITS (continued)

B 2.0 SAFETY LIMITS (SLs)

B 2.1.1 Reactor Core SLs (Analog)

BASES

BACKGROUND

GDC 10 (Ref. 1) requires and SLs ensure that specified acceptable fuel design limits are not exceeded during steady state operation, normal operation transients, and anticipated operational occurrences (AOOs). This is accomplished by having a departure from nucleate boiling (DNB) design basis, which corresponds to a 95% probability at a 95% confidence level (95/95 DNB criterion) that DNB will not occur and by requiring that fuel centerline temperature stays below the melting temperature.

The restrictions of this SL prevent overheating of the fuel and cladding and possible cladding perforation that would result in the release of fission products to the reactor coolant. Overheating of the fuel is prevented by maintaining the steady state peak linear heat rate (LHR) below the level at which fuel centerline melting occurs. Overheating of the fuel cladding is prevented by restricting fuel operation to within the nucleate boiling regime, where the heat transfer coefficient is large and the cladding surface temperature is slightly above the coolant saturation temperature.

Fuel centerline melting occurs when the local LHR, or power peaking, in a region of the fuel is high enough to cause the fuel centerline temperature to reach the melting point of the fuel. Expansion of the pellet upon centerline melting may cause the pellet to stress the cladding to the point of failure, allowing an uncontrolled release of activity to the reactor coolant.

Operation above the boundary of the nucleate boiling regime could result in excessive cladding temperature because of the onset of DNB and the resultant sharp reduction in heat transfer coefficient. Inside the steam film, high cladding temperatures are reached, and a cladding water (zirconium water) reaction may take place. This chemical reaction results in oxidation of the fuel cladding to a structurally weaker form. This weaker form may lose its integrity, resulting in an uncontrolled release of activity to the reactor coolant.

The Reactor Protective System (RPS), in combination with the LCOs, is designed to prevent any anticipated combination of transient conditions for Reactor Coolant System (RCS) temperature, pressure, and THERMAL POWER level that would result in a violation of the reactor core SLs.

BASES

APPLICABLE SAFETY ANALYSES

The fuel cladding must not sustain damage as a result of normal operation and AOOs. The reactor core SLs are established to preclude violation of the following fuel design criteria:

a. There must be at least 95% probability at a 95% confidence level (the 95/95 DNB criterion) that the hot fuel rod in the core does not experience a DNB and

b. The hot fuel pellet in the core must not experience fuel centerline melting.

The RPS setpoints, LCO 3.3.1, "Reactor Protective System (RPS) Instrumentation," in combination with all the LCOs, are designed to prevent any anticipated combination of transient conditions for RCS temperature, pressure, and THERMAL POWER level that would result in a departure from nucleate boiling ratio (DNBR) of less than the DNBR limit and preclude the existence of flow instabilities.

Automatic enforcement of these reactor core SLs is provided by the following functions:

a. Pressurizer Pressure High trip,

b. Variable High Power trip,

c. Power Rate of Change - High trip,

d. Reactor Coolant Flow - Low trip,

e. Steam Generator Pressure - Low trip,

f. Steam Generator Level - Low trip,

g. Axial Power Distribution - High trip,

h. Thermal Margin/Low Pressure trip,

i. Steam Generator Pressure Difference trip, and

j. Steam Generator Safety Valves.

The SL represents a design requirement for establishing the RPS trip setpoints identified previously. LCO 3.2.1, "Linear Heat Rate (LHR)," and LCO 3.2.5, "AXIAL SHAPE INDEX (ASI)," or the assumed initial conditions of the safety analyses (as indicated in the FSAR, Ref. 2) provide more restrictive limits to ensure that the SLs are not exceeded.

BASES

SAFETY LIMITS

The curves provided in Figure B 2.1.1-1 show the loci of points of THERMAL POWER, pressurizer pressure, and highest operating loop cold leg temperature, for which the minimum DNBR is not less than the safety analysis limit. SL 2.1.1.2 ensures that fuel centerline temperature remains below melting.

SL 2.1.1.2 ensures that fuel centerline temperature remains below the fuel melt temperature of [5080]°F during normal operating conditions or design AOOs with adjustments for burnup and burnable poison. An adjustment of [58°F per 10,000 MWD/MTU] has been established in [Topical Report CEN-386-P-A] (Ref. 3) and adjustments for burnable poisons are established based on [Topical Reports CENPD-275-P] (Ref. 4) and [CENPD-382-P-A] (Ref.5).

APPLICABILITY

SL 2.1.1 only applies in MODES 1 and 2 because these are the only MODES in which the reactor is critical. Automatic protection functions are required to be OPERABLE during MODES 1 and 2 to ensure operation within the reactor core SLs. The steam generator safety valves or automatic protection actions serve to prevent RCS heatup to the reactor core SL conditions or to initiate a reactor trip function, which forces the unit into MODE 3. Setpoints for the reactor trip functions are specified in LCO 3.3.1.

In MODES 3, 4, 5, and 6, Applicability is not required, since the reactor is not generating significant THERMAL POWER.

SAFETY LIMIT VIOLATIONS

The following SL violation responses are applicable to the reactor core SLs.

<u>2.2.1</u>

If SL 2.1.1 is violated, the requirement to go to MODE 3 places the unit in a MODE in which this SL is not applicable.

The allowed Completion Time of 1 hour recognizes the importance of bringing the unit to a MODE of operation where this SL is not applicable and reduces the probability of fuel damage.

BASES

REFERENCES

1. 10 CFR 50, Appendix A, GDC 10, 1988.
2. FSAR, Section [ ].
3. [Topical Report CEN-386-P-A, “Verification of the Acceptability of a 1-Pin Burnup Limit of 60 MWD/kgU for Combustion Engineering 16x16 PWR Fuel,” August 1992.]
4. [Topical Report CENPD-275-P, Revision 1-P-A, “CE Methodology for Core Designs Containing Gadolini-Urania Burnable Absorbers,” May 1988.]
5. [Topical Report CENPD-382-P-A, “Methodology for Core Designs Containing Erbium Burnable Absorbers,” August 1993.]

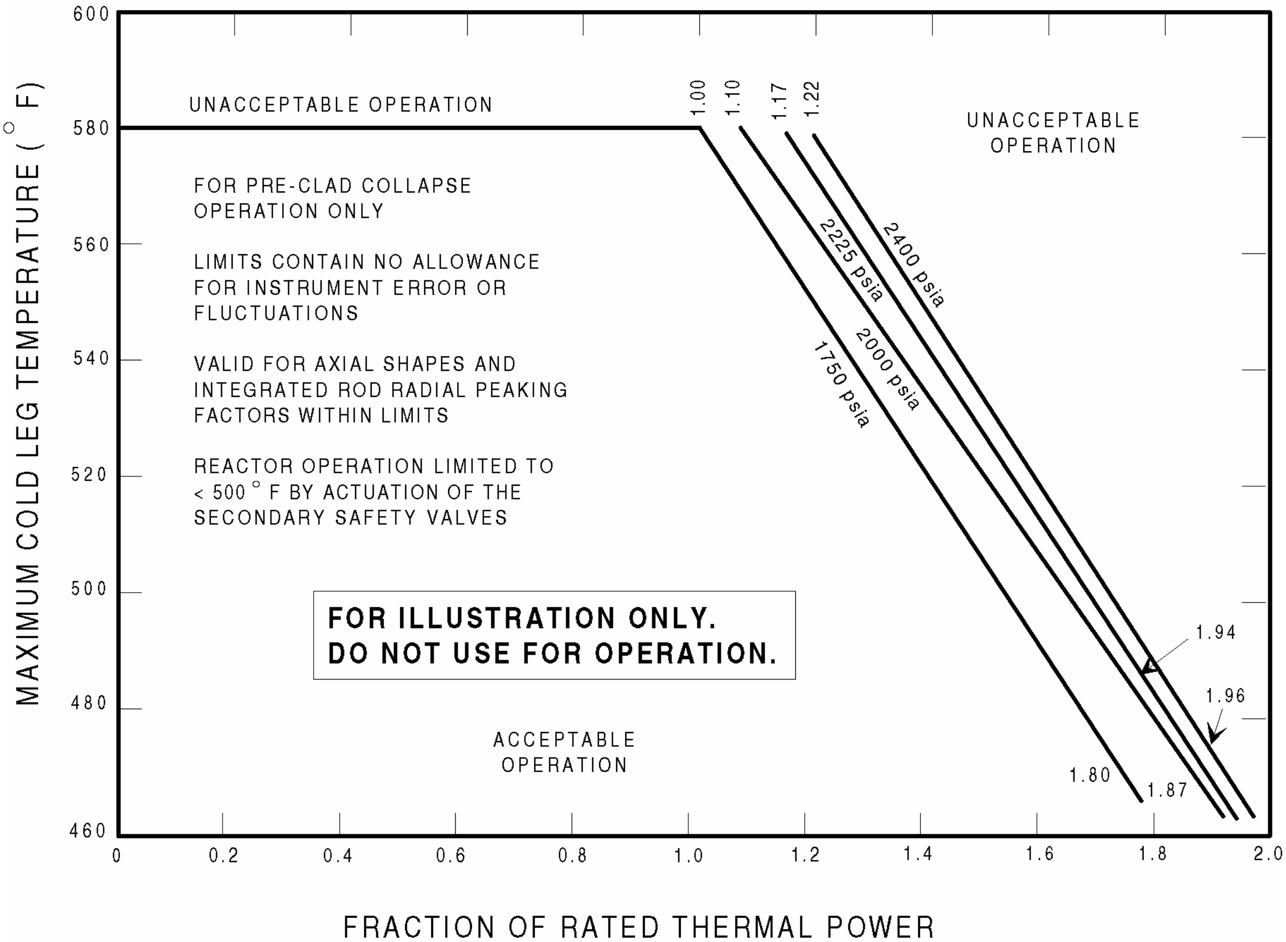


Figure 2.1.1-1 (page 1 of 1)
Reactor Core Thermal Margin Safety Limit

B 2.0 SAFETY LIMITS (SLs)

B 2.1.2 Reactor Coolant System (RCS) Pressure SL (Analog)

BASES

BACKGROUND	The SL on RCS pressure protects the integrity of the RCS against overpressurization. In the event of fuel cladding failure, fission products are released into the reactor coolant. The RCS then serves as the primary barrier in preventing the release of fission products into the atmosphere. By establishing an upper limit on RCS pressure, continued RCS integrity is ensured. According to 10 CFR 50, Appendix A, GDC 14, "Reactor Coolant Pressure Boundary," and GDC 15, "Reactor Coolant System Design" (Ref. 1), the reactor coolant pressure boundary (RCPB) design conditions are not to be exceeded during normal operation and anticipated operational occurrences (AOOs). Also, according to GDC 28 (Ref. 1), "Reactivity Limits," reactivity accidents, including rod ejection, do not result in damage to the RCPB greater than limited local yielding. The design pressure of the RCS is 2500 psia. During normal operation and AOOs, the RCS pressure is kept from exceeding the design pressure by more than 10%, in accordance with Section III of the ASME Code (Ref. 2). To ensure system integrity, all RCS components are hydrostatically tested at 125% of design pressure, according to the ASME Code requirements prior to initial operation, when there is no fuel in the core. Following inception of unit operation, RCS components shall be pressure tested, in accordance with the requirements of ASME Code, Section XI (Ref. 3). Overpressurization of the RCS could result in a breach of the RCPB. If this occurs in conjunction with a fuel cladding failure, fission products could enter the containment atmosphere, raising concerns relative to limits on radioactive releases specified in 10 CFR 100, "Reactor Site Criteria" (Ref. 4).
APPLICABLE SAFETY ANALYSES	The RCS pressurizer safety valves, the main steam safety valves (MSSVs), and the Reactor Pressure - High trip have settings established to ensure that the RCS pressure SL will not be exceeded. The RCS pressurizer safety valves are sized to prevent system pressure from exceeding the design pressure by more than 10%, in accordance with Section III of the ASME Code for Nuclear Power Plant Components (Ref. 2). The transient that establishes the required relief capacity, and

BASES

APPLICABLE SAFETY ANALYSES (continued)

hence the valve size requirements and lift settings, is a [complete loss of external load without a direct reactor trip]. During the transient, no control actions are assumed except that the safety valves on the secondary plant are assumed to open when the steam pressure reaches the secondary plant safety valve settings, and nominal feedwater supply is maintained.

The Reactor Protective System (RPS) trip setpoints (LCO 3.3.1, "Reactor Protective System (RPS) Instrumentation"), together with the settings of the MSSVs (LCO 3.7.1, "Main Steam Safety Valves (MSSVs)") and the pressurizer safety valves, provide pressure protection for normal operation and AOOs. In particular, the Pressurizer Pressure - High trip setpoint is specifically set to provide protection against overpressurization (Ref. 5). Safety analyses for both the Pressure - High trip and the RCS pressurizer safety valves are performed, using conservative assumptions relative to pressure control devices.

More specifically, no credit is taken for operation of any of the following:

a. Pressurizer power operated relief valves (PORVs),

b. Steam Bypass Control System,

c. Pressurizer Level Control System, or

d. Pressurizer Pressure Control System.

SAFETY LIMITS

The maximum transient pressure allowable in the RCS pressure vessel under the ASME Code, Section III, is 110% of design pressure. The maximum transient pressure allowable in the RCS piping, valves, and fittings under [USAS, Section B31.1 (Ref. 6)], is 120% of design pressure. The most limiting of these two allowances is the 110% of design pressure; therefore, the SL on maximum allowable RCS pressure is established at 2750 psia.

APPLICABILITY

SL 2.1.2 applies in MODES 1, 2, 3, 4, and 5 because this SL could be approached or exceeded in these MODES due to overpressurization events. The SL is not applicable in MODE 6 because the reactor vessel head closure bolts are not fully tightened, making it unlikely that the RCS can be pressurized.

BASES

SAFETY LIMIT VIOLATIONS

The following SL violation responses are applicable to the RCS pressure SL.

2.2.2.1

If the RCS pressure SL is violated when the reactor is in MODE 1 or 2, the requirement is to restore compliance and be in MODE 3 within 1 hour.

With RCS pressure greater than the value specified in SL 2.1.2 in MODE 1 or 2, the pressure must be reduced to below this value. A pressure greater than the value specified in SL 2.1.2 exceeds 110% of the RCS design pressure and may challenge system integrity.

The allowed Completion Time of 1 hour provides the operator time to complete the necessary actions to reduce RCS pressure by terminating the cause of the pressure increase, removing mass or energy from the RCS, or a combination of these actions, and to establish MODE 3 conditions.

2.2.2.2

If the RCS pressure SL is exceeded in MODE 3, 4, or 5, RCS pressure must be restored to within the SL value within 5 minutes.

Exceeding the RCS pressure SL in MODE 3, 4, or 5 is potentially more severe than exceeding this SL in MODE 1 or 2, since the reactor vessel temperature may be lower and the vessel material, consequently, less ductile. As such, pressure must be reduced to less than the SL within 5 minutes. This action does not require reducing MODES, since this would require reducing temperature, which would compound the problem by adding thermal gradient stresses to the existing pressure stress.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 14, GDC 15, and GDC 28.
2. ASME, Boiler and Pressure Vessel Code, Section III, Article NB-7000.
3. ASME, Boiler and Pressure Vessel Code, Section XI, Article IWX-5000.
4. 10 CFR 100.
5. FSAR, Section [ ].

[6. ASME, USAS B31.1, Standard Code for Pressure Piping, 1967.]

B 2.0 SAFETY LIMITS (SLs)

B 2.1.1 Reactor Core SLs (Digital)

BASES

BACKGROUND

GDC 10 (Ref. 1) requires and SLs ensure that specified acceptable fuel design limits are not exceeded during steady state operation, normal operational transients, and anticipated operational occurrences (AOOs). This is accomplished by having a departure from nucleate boiling (DNB) design basis, which corresponds to a 95% probability at a 95% confidence level (95/95 DNB criterion) that DNB will not occur and by requiring that fuel centerline temperature stays below the melting temperature.

The restrictions of this SL prevent overheating of the fuel and cladding and possible cladding perforation that would result in the release of fission products to the reactor coolant. Overheating of the fuel is prevented by maintaining the steady state, peak linear heat rate (LHR) below the level at which fuel centerline melting occurs. Overheating of the fuel cladding is prevented by restricting fuel operation to within the nucleate boiling regime, where the heat transfer coefficient is large and the cladding surface temperature is slightly above the coolant saturation temperature.

Fuel centerline melting occurs when the local LHR, or power peaking, in a region of the fuel is high enough to cause the fuel centerline temperature to reach the melting point of the fuel. Expansion of the pellet upon centerline melting may cause the pellet to stress the cladding to the point of failure, allowing an uncontrolled release of activity to the reactor coolant.

Operation above the boundary of the nucleate boiling regime could result in excessive cladding temperature because of the onset of DNB and the resultant sharp reduction in the heat transfer coefficient. Inside the steam film, high cladding temperatures are reached, and a cladding water (zirconium water) reaction may take place. This chemical reaction results in oxidation of the fuel cladding to a structurally weaker form. This weaker form may lose its integrity, resulting in an uncontrolled release of activity to the reactor coolant.

The Reactor Protective System (RPS), in combination with the LCOs, is designed to prevent any anticipated combination of transient conditions for Reactor Coolant System (RCS) temperature, pressure, and THERMAL POWER level that would result in a violation of the reactor core SLs.

BASES

APPLICABLE SAFETY ANALYSES

The fuel cladding must not sustain damage as a result of normal operation and AOOs. The reactor core SLs are established to preclude violation of the following fuel design criteria:

a. There must be at least a 95% probability at a 95% confidence level (95/95 DNB criterion) that the hot fuel rod in the core does not experience DNB and

b. The hot fuel pellet in the core must not experience centerline fuel melting.

The RPS setpoints, LCO 3.3.1, "Reactor Protective System (RPS) Instrumentation," in combination with all the LCOs, are designed to prevent any anticipated combination of transient conditions for RCS temperature, pressure, and THERMAL POWER level that would result in a departure from nucleate boiling ratio (DNBR) of less than the DNBR limit and preclude the existence of flow instabilities.

Automatic enforcement of these reactor core SLs is provided by the following functions:

a. Pressurizer Pressure - High trip,

b. Pressurizer Pressure - Low trip,

c. Linear Power Level - High trip,

d. Steam Generator Pressure - Low trip,

e. Local Power Density - High trip,

f. DNBR - Low trip,

g. Steam Generator Level - Low trip,

h. Reactor Coolant Flow - Low trip, and

i. Steam Generator Safety Valves.

The limitation that the average enthalpy in the hot leg be less than or equal to the enthalpy of saturated liquid also ensures that the ΔT measured by instrumentation used in the protection system design as a measure of the core power is proportional to core power.

BASES

APPLICABLE SAFETY ANALYSES (continued)

The SL represents a design requirement for establishing the protection system trip setpoints identified previously. LCO 3.2.1, "Linear Heat Rate (LHR)," and LCO 3.2.4, "Departure From Nucleate Boiling Ratio (DNBR)," or the assumed initial conditions of the safety analyses (as indicated in the FSAR, Ref. 2) provide more restrictive limits to ensure that the SLs are not exceeded.

SAFETY LIMITS

SL 2.1.1.1 and SL 2.1.1.2 ensure that the minimum DNBR is not less than the safety analyses limit and that fuel centerline temperature remains below melting.

The minimum value of the DNBR during normal operation and design basis AOOs is limited to [1.19], based on a statistical combination of CE-1 CHF correlation and engineering factor uncertainties, and is established as an SL. Additional factors such as rod bow and spacer grid size and placement will determine the limiting safety system settings required to ensure that the SL is maintained. Maintaining the dynamically adjusted peak LHR to ≤ 21 kW/ft ensures that fuel centerline melt will not occur during normal operating conditions or design AOOs.

SL 2.1.1.2 ensures that fuel centerline temperature remains below the fuel melt temperature of [5080]°F during normal operating conditions or design AOOs with adjustments for burnup and burnable poison. An adjustment of [58°F per 10,000 MWD/MTU] has been established in [Topical Report CEN-386-P-A] (Ref. 3) and adjustments for burnable poisons are established based on [Topical Reports CENPD-275-P] (Ref. 4) and [CENPD-382-P-A] (Ref.5).

APPLICABILITY

SL 2.1.1.1 and SL 2.1.1.2 only apply in MODES 1 and 2 because these are the only MODES in which the reactor is critical. Automatic protection functions are required to be OPERABLE during MODES 1 and 2 to ensure operation within the reactor core SLs. The steam generator safety valves or automatic protection actions serve to prevent RCS heatup to the reactor core SL conditions or to initiate a reactor trip function, which forces the unit into MODE 3. Setpoints for the reactor trip functions are specified in LCO 3.3.1.

In MODES 3, 4, 5, and 6, Applicability is not required, since the reactor is not generating significant THERMAL POWER.

BASES

SAFETY LIMIT VIOLATIONS	The following SL violation responses are applicable to the reactor core SLs. If SL 2.1.1.1 or SL 2.1.1.2 is violated, the requirement to go to MODE 3 places the unit in a MODE in which this SL is not applicable. The allowed Completion Time of 1 hour recognizes the importance of bringing the unit to a MODE where this SL is not applicable and reduces the probability of fuel damage.
REFERENCES	1. 10 CFR 50, Appendix A, GDC 10, 1988. 2. FSAR, Section [ ]. 3. [Topical Report CEN-386-P-A, “Verification of the Acceptability of a 1-Pin Burnup Limit of 60 MWD/kgU for Combustion Engineering 16x16 PWR Fuel,” August 1992.] 4. [Topical Report CENPD-275-P, Revision 1-P-A, “CE Methodology for Core Designs Containing Gadolini-Urania Burnable Absorbers,” May 1988.] 5. [Topical Report CENPD-382-P-A, “Methodology for Core Designs Containing Erbium Burnable Absorbers,” August 1993.]

B 2.0 SAFETY LIMITS (SLs)

B 2.1.2 Reactor Coolant System (RCS) Pressure SL (Digital)

BASES

BACKGROUND

The SL on RCS pressure protects the integrity of the RCS against overpressurization. In the event of fuel cladding failure, fission products are released into the reactor coolant. The RCS then serves as the primary barrier in preventing the release of fission products into the atmosphere. By establishing an upper limit on RCS pressure, continued RCS integrity is ensured. According to 10 CFR 50, Appendix A, GDC 14, "Reactor Coolant Pressure Boundary," and GDC 15, "Reactor Coolant System Design" (Ref. 1), the reactor coolant pressure boundary (RCPB) design conditions are not to be exceeded during normal operation and anticipated operational occurrences (AOOs). Also, according to GDC 28 (Ref. 1), "Reactivity Limits," reactivity accidents, including rod ejection, do not result in damage to the RCPB greater than limited local yielding.

The design pressure of the RCS is 2500 psia. During normal operation and AOOs, the RCS pressure is kept from exceeding the design pressure by more than 10%, in accordance with Section III of the ASME Code (Ref. 2). To ensure system integrity, all RCS components are hydrostatically tested at 125% of design pressure, according to the ASME Code requirements prior to initial operation, when there is no fuel in the core. Following inception of unit operation, RCS components shall be pressure tested, in accordance with the requirements of ASME Code, Section XI (Ref. 3).

Overpressurization of the RCS could result in a breach of the RCPB. If this occurs in conjunction with a fuel cladding failure, fission products could enter the containment atmosphere, raising concerns relative to limits on radioactive releases specified in 10 CFR 100, "Reactor Site Criteria" (Ref. 4).

APPLICABLE SAFETY ANALYSES

The RCS pressurizer safety valves, the main steam safety valves (MSSVs), and the Reactor Pressure - High trip have settings established to ensure that the RCS pressure SL will not be exceeded.

The RCS pressurizer safety valves are sized to prevent system pressure from exceeding the design pressure by more than 10%, in accordance with Section III of the ASME Code for Nuclear Power Plant Components (Ref. 2). The transient that establishes the required relief capacity, and hence the valve size requirements and lift settings, is a [complete loss of

BASES

APPLICABLE SAFETY ANALYSES (continued)

external load without a direct reactor trip]. During the transient, no control actions are assumed except that the safety valves on the secondary plant are assumed to open when the steam pressure reaches the secondary plant safety valve settings, and nominal feedwater supply is maintained.

The Reactor Protective System (RPS) trip setpoints (LCO 3.3.1, "Reactor Protective System (RPS) Instrumentation"), together with the settings of the MSSVs (LCO 3.7.1, "Main Steam Safety Valves (MSSVs)") and the pressurizer safety valves, provide pressure protection for normal operation and AOOs. In particular, the Pressurizer Pressure - High Trip setpoint is specifically set to provide protection against overpressurization (Ref. 5). Safety analyses for both the Pressure - High Trip and the RCS pressurizer safety valves are performed, using conservative assumptions relative to pressure control devices.

More specifically, no credit is taken for operation of any of the following:

a. Pressurizer power operated relief valves (PORVs),

b. Steam Bypass Control System,

c. Pressurizer Level Control System, or

d. Pressurizer Pressure Control System.

SAFETY LIMITS

The maximum transient pressure allowable in the RCS pressure vessel under the ASME Code, Section III, is 110% of design pressure. The maximum transient pressure allowable in the RCS piping, valves, and fittings under [USAS, Section B31.1 (Ref. 6)], is 120% of design pressure. The most limiting of these two allowances is the 110% of design pressure; therefore, the SL on maximum allowable RCS pressure is established at 2750 psia.

APPLICABILITY

SL 2.1.2 applies in MODES 1, 2, 3, 4, and 5 because this SL could be approached or exceeded in these MODES due to overpressurization events. The SL is not applicable in MODE 6 because the reactor vessel head closure bolts are not fully tightened, making it unlikely that the RCS can be pressurized.

BASES

SAFETY LIMIT VIOLATIONS

The following SL violation responses are applicable to the RCS pressure SL.

2.2.2.1

If the RCS pressure SL is violated when the reactor is in MODE 1 or 2, the requirement is to restore compliance and be in MODE 3 within 1 hour.

With RCS pressure greater than the value specified in SL 2.1.2 in MODE 1 or 2, the pressure must be reduced to below this value. A pressure greater that the value specified in SL 2.1.2 exceeds 110% of the RCS design pressure and may challenge system integrity.

The allowed Completion Time of 1 hour provides the operator time to complete the necessary actions to reduce RCS pressure by terminating the cause of the pressure increase, removing mass or energy from the RCS, or a combination of these actions, and to establish MODE 3 conditions.

2.2.2.2

If the RCS pressure SL is exceeded in MODE 3, 4, or 5, RCS pressure must be restored to within the SL value within 5 minutes.

Exceeding the RCS pressure SL in MODE 3, 4, or 5 is potentially more severe than exceeding this SL in MODE 1 or 2, since the reactor vessel temperature may be lower and the vessel material, consequently, less ductile. As such, pressure must be reduced to less than the SL within 5 minutes. This action does not require reducing MODES, since this would require reducing temperature, which would compound the problem by adding thermal gradient stresses to the existing pressure stress.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 14, GDC 15, and GDC 28.

2. ASME, Boiler and Pressure Vessel Code, Section III, Article NB-7000.

3. ASME, Boiler and Pressure Vessel Code, Section XI, Article IWX-5000.

4. 10 CFR 100.

5. FSAR, Section [ ].

[6. ASME, USAS B31.1, Standard Code for Pressure Piping, 1967.]

B 3.0 LIMITING CONDITION FOR OPERATION (LCO) APPLICABILITY

BASES

LCOs	LCO 3.0.1 through LCO 3.0.8 establish the general requirements applicable to all Specifications and apply at all times unless otherwise stated.
LCO 3.0.1	LCO 3.0.1 establishes the Applicability statement within each individual Specification as the requirement for when the LCO is required to be met (i.e., when the unit is in the MODES or other specified conditions of the Applicability statement of each Specification).

LCO 3.0.2

LCO 3.0.2 establishes that upon discovery of a failure to meet an LCO, the associated ACTIONS shall be met. The Completion Time of each Required Action for an ACTIONS Condition is applicable from the point in time that an ACTIONS Condition is entered. The Required Actions establish those remedial measures that must be taken within specified Completion Times when the requirements of an LCO are not met. This Specification establishes that:

a. Completion of the Required Actions within the specified Completion Times constitutes compliance with a Specification and

b. Completion of the Required Actions is not required when an LCO is met within the specified Completion Time, unless otherwise specified.

There are two basic types of Required Actions. The first type of Required Action specifies a time limit in which the LCO must be met. This time limit is the Completion Time to restore an inoperable system or component to OPERABLE status or to restore variables to within specified limits. If this type of Required Action is not completed within the specified Completion Time, a shutdown may be required to place the unit in a MODE or condition in which the Specification is not applicable. (Whether stated as a Required Action or not, correction of the entered Condition is an action that may always be considered upon entering ACTIONS.) The second type of Required Action specifies the remedial measures that permit continued operation of the unit that is not further restricted by the Completion Time. In this case, compliance with the Required Actions provides an acceptable level of safety for continued operation.

Completing the Required Actions is not required when an LCO is met or is no longer applicable, unless otherwise stated in the individual Specifications.

BASES

LCO 3.0.2 (continued)

The nature of some Required Actions of some Conditions necessitates that, once the Condition is entered, the Required Actions must be completed even though the associated Conditions no longer exist. The individual LCO's ACTIONS specify the Required Actions where this is the case. An example of this is in LCO 3.4.3, "RCS Pressure and Temperature (P/T) Limits."

The Completion Times of the Required Actions are also applicable when a system or component is removed from service intentionally. The reasons for intentionally relying on the ACTIONS include, but are not limited to, performance of Surveillances, preventive maintenance, corrective maintenance, or investigation of operational problems. Entering ACTIONS for these reasons must be done in a manner that does not compromise safety. Intentional entry into ACTIONS should not be made for operational convenience. Additionally, if intentional entry into ACTIONS would result in redundant equipment being inoperable, alternatives should be used instead. Doing so limits the time both subsystems/trains of a safety function are inoperable and limits the time conditions exist which may result in LCO 3.0.3 being entered. Individual Specifications may specify a time limit for performing an SR when equipment is removed from service or bypassed for testing. In this case, the Completion Times of the Required Actions are applicable when this time limit expires, if the equipment remains removed from service or bypassed.

When a change in MODE or other specified condition is required to comply with Required Actions, the unit may enter a MODE or other specified condition in which another Specification becomes applicable. In this case, the Completion Times of the associated Required Actions would apply from the point in time that the new Specification becomes applicable and the ACTIONS Condition(s) are entered.

LCO 3.0.3

LCO 3.0.3 establishes the actions that must be implemented when an LCO is not met and either:

a. An associated Required Action and Completion Time is not met and no other Condition applies or

b. The condition of the unit is not specifically addressed by the associated ACTIONS. This means that no combination of Conditions stated in the ACTIONS can be made that exactly corresponds to the actual condition of the unit. Sometimes, possible combinations of Conditions are such that entering LCO 3.0.3 is warranted; in such cases, the ACTIONS specifically state a Condition corresponding to such combinations and also that LCO 3.0.3 be entered immediately.

BASES

LCO 3.0.3 (continued)

This Specification delineates the time limits for placing the unit in a safe MODE or other specified condition when operation cannot be maintained within the limits for safe operation as defined by the LCO and its ACTIONS. It is not intended to be used as an operational convenience that permits routine voluntary removal of redundant systems or components from service in lieu of other alternatives that would not result in redundant systems or components being inoperable.

Upon entering LCO 3.0.3, 1 hour is allowed to prepare for an orderly shutdown before initiating a change in unit operation. This includes time to permit the operator to coordinate the reduction in electrical generation with the load dispatcher to ensure the stability and availability of the electrical grid. The time limits specified to reach lower MODES of operation permit the shutdown to proceed in a controlled and orderly manner that is well within the specified maximum cooldown rate and within the capabilities of the unit, assuming that only the minimum required equipment is OPERABLE. This reduces thermal stresses on components of the Reactor Coolant System and the potential for a plant upset that could challenge safety systems under conditions to which this Specification applies. The use and interpretation of specified times to complete the actions of LCO 3.0.3 are consistent with the discussion of Section 1.3, Completion Times.

A unit shutdown required in accordance with LCO 3.0.3 may be terminated and LCO 3.0.3 exited if any of the following occurs:

a. The LCO is now met,

b. A Condition exists for which the Required Actions have now been performed, or

c. ACTIONS exist that do not have expired Completion Times. These Completion Times are applicable from the point in time that the Condition is initially entered and not from the time LCO 3.0.3 is exited.

The time limits of LCO 3.0.3 allow 37 hours for the unit to be in MODE 5 when a shutdown is required during MODE 1 operation. If the unit is in a lower MODE of operation when a shutdown is required, the time limit for reaching the next lower MODE applies. If a lower MODE is reached in less time than allowed, however, the total allowable time to reach

BASES

LCO 3.0.3 (continued)

MODE 5, or other applicable MODE, is not reduced. For example, if MODE 3 is reached in 2 hours, then the time allowed for reaching MODE 4 is the next 11 hours, because the total time for reaching MODE 4 is not reduced from the allowable limit of 13 hours. Therefore, if remedial measures are completed that would permit a return to MODE 1, a penalty is not incurred by having to reach a lower MODE of operation in less than the total time allowed.

In MODES 1, 2, 3, and 4, LCO 3.0.3 provides actions for Conditions not covered in other Specifications. The requirements of LCO 3.0.3 do not apply in MODES 5 and 6 because the unit is already in the most restrictive Condition required by LCO 3.0.3. The requirements of LCO 3.0.3 do not apply in other specified conditions of the Applicability (unless in MODE 1, 2, 3, or 4) because the ACTIONS of individual Specifications sufficiently define the remedial measures to be taken.

Exceptions to LCO 3.0.3 are provided in instances where requiring a unit shutdown, in accordance with LCO 3.0.3, would not provide appropriate remedial measures for the associated condition of the unit. An example of this is in LCO 3.7.16, "Fuel Storage Pool Water Level." LCO 3.7.16 has an Applicability of "During movement of irradiated fuel assemblies in the fuel storage pool." Therefore, this LCO can be applicable in any or all MODES. If the LCO and the Required Actions of LCO 3.7.16 are not met while in MODE 1, 2, or 3, there is no safety benefit to be gained by placing the unit in a shutdown condition. The Required Action of LCO 3.7.16 of "Suspend movement of irradiated fuel assemblies in fuel storage pool" is the appropriate Required Action to complete in lieu of the actions of LCO 3.0.3. These exceptions are addressed in the individual Specifications.

[The requirement to be in MODE 4 in 13 hours is plant specific and depends on the ability to cool the pressurizer and degas.]

LCO 3.0.4

LCO 3.0.4 establishes limitations on changes in MODES or other specified conditions in the Applicability when an LCO is not met. It allows placing the unit in a MODE or other specified condition stated in that Applicability (e.g., the Applicability desired to be entered) when unit conditions are such that the requirements of the LCO would not be met, in accordance with LCO 3.0.4.a, LCO 3.0.4.b, or LCO 3.0.4.c.

BASES

LCO 3.0.4 (continued)

LCO 3.0.4.a allows entry into a MODE or other specified condition in the Applicability with the LCO not met when the associated ACTIONS to be entered permit continued operation in the MODE or other specified condition in the Applicability for an unlimited period of time. Compliance with Required Actions that permit continued operation of the unit for an unlimited period of time in a MODE or other specified condition provides an acceptable level of safety for continued operation. This is without regard to the status of the unit before or after the MODE change. Therefore, in such cases, entry into a MODE or other specified condition in the Applicability may be made in accordance with the provisions of the Required Actions.

LCO 3.0.4.b allows entry into a MODE or other specified condition in the Applicability with the LCO not met after performance of a risk assessment addressing inoperable systems and components, consideration of the results, determination of the acceptability of entering the MODE or other specified condition in the Applicability, and establishment of risk management actions, if appropriate.

The risk assessment may use quantitative, qualitative, or blended approaches, and the risk assessment will be conducted using the plant program, procedures, and criteria in place to implement 10 CFR 50.65(a)(4), which requires that risk impacts of maintenance activities to be assessed and managed. The risk assessment, for the purposes of LCO 3.0.4.b, must take into account all inoperable Technical Specification equipment regardless of whether the equipment is included in the normal 10 CFR 50.65(a)(4) risk assessment scope. The risk assessments will be conducted using the procedures and guidance endorsed by Regulatory Guide 1.182, “Assessing and Managing Risk Before Maintenance Activities at Nuclear Power Plants.” Regulatory Guide 1.182 endorses the guidance in Section 11 of NUMARC 93-01, “Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants.” These documents address general guidance for conduct of the risk assessment, quantitative and qualitative guidelines for establishing risk management actions, and example risk management actions. These include actions to plan and conduct other activities in a manner that controls overall risk, increased risk awareness by shift and management personnel, actions to reduce the duration of the condition, actions to minimize the magnitude of risk increases (establishment of backup success paths or compensatory measures), and determination that the proposed MODE change is acceptable. Consideration should also be given to the probability of completing restoration such that the requirements of the LCO would be met prior to the expiration of ACTIONS Completion Times that would require exiting the Applicability.

BASES

LCO 3.0.4 (continued)

LCO 3.0.4.b may be used with single, or multiple systems and components unavailable. NUMARC 93-01 provides guidance relative to consideration of simultaneous unavailability of multiple systems and components.

The results of the risk assessment shall be considered in determining the acceptability of entering the MODE or other specified condition in the Applicability, and any corresponding risk management actions. The LCO 3.0.4.b risk assessments do not have to be documented.

The Technical Specifications allow continued operation with equipment unavailable in MODE 1 for the duration of the Completion Time. Since this is allowable, and since in general the risk impact in that particular MODE bounds the risk of transitioning into and through the applicable MODES or other specified conditions in the Applicability of the LCO, the use of the LCO 3.0.4.b allowance should be generally acceptable, as long as the risk is assessed and managed as stated above. However, there is a small subset of systems and components that have been determined to be more important to risk and use of the LCO 3.0.4.b allowance is prohibited. The LCOs governing these systems and components contain Notes prohibiting the use of LCO 3.0.4.b by stating that LCO 3.0.4.b is not applicable.

LCO 3.0.4.c allows entry into a MODE or other specified condition in the Applicability with the LCO not met based on a Note in the Specification which states LCO 3.0.4.c is applicable. These specific allowances permit entry into MODES or other specified conditions in the Applicability when the associated ACTIONS to be entered do not provide for continued operation for an unlimited period of time and a risk assessment has not been performed. This allowance may apply to all the ACTIONS or to a specific Required Action of a Specification. The risk assessments performed to justify the use of LCO 3.0.4.b usually only consider systems and components. For this reason, LCO 3.0.4.c is typically applied to Specifications which describe values and parameters (e.g., [Containment Air Temperature, Containment Pressure, MCPR, Moderator Temperature Coefficient]), and may be applied to other Specifications based on NRC plant specific approval.

The provisions of this Specification should not be interpreted as endorsing the failure to exercise the good practice of restoring systems or components to OPERABLE status before entering an associated MODE or other specified condition in the Applicability.

BASES

LCO 3.0.4 (continued)

The provisions of LCO 3.0.4 shall not prevent changes in MODES or other specified conditions in the Applicability that are required to comply with ACTIONS. In addition, the provisions of LCO 3.0.4 shall not prevent changes in MODES or other specified conditions in the Applicability that result from any unit shutdown. In this context, a unit shutdown is defined as a change in MODE or other specified condition in the Applicability associated with transitioning from MODE 1 to MODE 2, MODE 2 to MODE 3, MODE 3 to MODE 4, and MODE 4 to MODE 5.

Upon entry into a MODE or other specified condition in the Applicability with the LCO not met, LCO 3.0.1 and LCO 3.0.2 require entry into the applicable Conditions and Required Actions until the Condition is resolved, until the LCO is met, or until the unit is not within the Applicability of the Technical Specification.

Surveillances do not have to be performed on the associated inoperable equipment (or on variables outside the specified limits), as permitted by SR 3.0.1. Therefore, utilizing LCO 3.0.4 is not a violation of SR 3.0.1 or SR 3.0.4 for any Surveillances that have not been performed on inoperable equipment. However, SRs must be met to ensure OPERABILITY prior to declaring the associated equipment OPERABLE (or variable within limits) and restoring compliance with the affected LCO.

LCO 3.0.5

LCO 3.0.5 establishes the allowance for restoring equipment to service under administrative controls when it has been removed from service or declared inoperable to comply with ACTIONS. The sole purpose of this Specification is to provide an exception to LCO 3.0.2 (e.g., to not comply with the applicable Required Action(s)) to allow the performance of required testing to demonstrate either:

a. The OPERABILITY of the equipment being returned to service or

b. The OPERABILITY of other equipment.

The administrative controls ensure the time the equipment is returned to service in conflict with the requirements of the ACTIONS is limited to the time absolutely necessary to perform the required testing to demonstrate OPERABILITY. This Specification does not provide time to perform any other preventive or corrective maintenance.

BASES

LCO 3.0.5 (continued)

An example of demonstrating the OPERABILITY of the equipment being returned to service is reopening a containment isolation valve that has been closed to comply with Required Actions and must be reopened to perform the required testing.

An example of demonstrating the OPERABILITY of other equipment is taking an inoperable channel or trip system out of the tripped condition to prevent the trip function from occurring during the performance of required testing on another channel in the other trip system. A similar example of demonstrating the OPERABILITY of other equipment is taking an inoperable channel or trip system out of the tripped condition to permit the logic to function and indicate the appropriate response during the performance of required testing on another channel in the same trip system.

LCO 3.0.6

LCO 3.0.6 establishes an exception to LCO 3.0.2 for supported systems that have a support system LCO specified in the Technical Specifications (TS). This exception is provided because LCO 3.0.2 would require that the Conditions and Required Actions of the associated inoperable supported system LCO be entered solely due to the inoperability of the support system. This exception is justified because the actions that are required to ensure the unit is maintained in a safe condition are specified in the support system LCO's Required Actions. These Required Actions may include entering the supported system's Conditions and Required Actions or may specify other Required Actions.

When a support system is inoperable and there is an LCO specified for it in the TS, the supported system(s) are required to be declared inoperable if determined to be inoperable as a result of the support system inoperability. However, it is not necessary to enter into the supported systems' Conditions and Required Actions unless directed to do so by the support system's Required Actions. The potential confusion and inconsistency of requirements related to the entry into multiple support and supported systems' LCOs' Conditions and Required Actions are eliminated by providing all the actions that are necessary to ensure the unit is maintained in a safe condition in the support system's Required Actions.

However, there are instances where a support system's Required Action may either direct a supported system to be declared inoperable or direct entry into Conditions and Required Actions for the supported system. This may occur immediately or after some specified delay to perform

BASES

LCO 3.0.6 (continued)

some other Required Action. Regardless of whether it is immediate or after some delay, when a support system's Required Action directs a supported system to be declared inoperable or directs entry into Conditions and Required Actions for a supported system, the applicable Conditions and Required Actions shall be entered in accordance with LCO 3.0.2.

Specification 5.5.15, "Safety Function Determination Program (SFDP)," ensures loss of safety function is detected and appropriate actions are taken. Upon entry into LCO 3.0.6, an evaluation shall be made to determine if loss of safety function exists. Additionally, other limitations, remedial actions, or compensatory actions may be identified as a result of the support system inoperability and corresponding exception to entering supported system Conditions and Required Actions. The SFDP implements the requirements of LCO 3.0.6.

Cross train checks to identify a loss of safety function for those support systems that support multiple and redundant safety systems are required. The cross train check verifies that the supported systems of the redundant OPERABLE support system are OPERABLE, thereby ensuring safety function is retained. [A loss of safety function may exist when a support system is inoperable, and:

a. A required system redundant to system(s) supported by the inoperable support system is also inoperable (EXAMPLE B 3.0.6-1),

b. A required system redundant to system(s) in turn supported by the inoperable supported system is also inoperable (EXAMPLE B 3.0.6-2), or

c. A required system redundant to support system(s) for the supported systems (a) and (b) above is also inoperable (EXAMPLE B 3.0.6-3).

<u>EXAMPLE B 3.0.6-1</u>

If System 2 of Train A is inoperable and System 5 of Train B is inoperable, a loss of safety function exists in supported System 5.

<u>EXAMPLE B 3.0.6-2</u>

If System 2 of Train A is inoperable, and System 11 of Train B is inoperable, a loss of safety function exists in System 11 which is in turn supported by System 5.

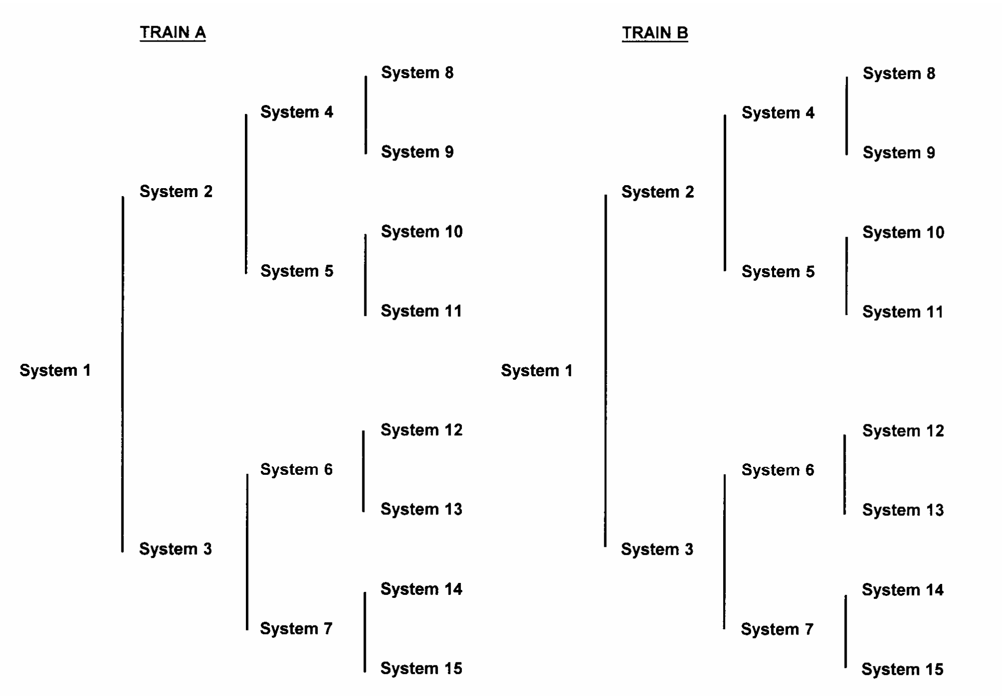
BASES

LCO 3.0.6 (continued)

EXAMPLE B 3.0.6-3

If System 2 of Train A is inoperable, and System 1 of Train B is inoperable, a loss of safety function exists in Systems 2, 4, 5, 8, 9, 10 and 11.]

If this evaluation determines that a loss of safety function exists, the appropriate Conditions and Required Actions of the LCO in which the loss of safety function exists are required to be entered.



[Figure B 3.0-1
Configuration of Trains and Systems]

This loss of safety function does not require the assumption of additional single failures or loss of offsite power. Since operations are being restricted in accordance with the ACTIONS of the support system, any resulting temporary loss of redundancy or single failure protection is taken into account. Similarly, the ACTIONS for inoperable offsite circuit(s) and inoperable diesel generator(s) provide the necessary restriction for cross train inoperabilities. This explicit cross train verification for inoperable AC electrical power sources also acknowledges that supported system(s) are not declared inoperable solely as a result of inoperability of a normal or emergency electrical power source (refer to the definition of OPERABILITY).

BASES

LCO 3.0.6 (continued)

When loss of safety function is determined to exist, and the SFDP requires entry into the appropriate Conditions and Required Actions of the LCO in which the loss of safety function exists, consideration must be given to the specific type of function affected. Where a loss of function is solely due to a single Technical Specification support system (e.g., loss of automatic start due to inoperable instrumentation, or loss of pump suction source due to low tank level) the appropriate LCO is the LCO for the support system. The ACTIONS for a support system LCO adequately address the inoperabilities of that system without reliance on entering its supported system LCO. When the loss of function is the result of multiple support systems, the appropriate LCO is the LCO for the supported system.

LCO 3.0.7

Special tests and operations are required at various times over the unit's life to demonstrate performance characteristics, to perform maintenance activities, and to perform special evaluations. Because TS normally preclude these tests and operations, special test exceptions (STEs) allow specified requirements to be changed or suspended under controlled conditions. STEs are included in applicable sections of the Specifications. Unless otherwise specified, all other TS requirements remain unchanged and in effect as applicable. This will ensure that all appropriate requirements of the MODE or other specified condition not directly associated with or required to be changed or suspended to perform the special test or operation will remain in effect.

The Applicability of an STE LCO represents a condition not necessarily in compliance with the normal requirements of the TS. Compliance with STE LCOs is optional.

A special test may be performed under either the provisions of the appropriate STE LCO or the other applicable TS requirements. If it is desired to perform the special test under the provisions of the STE LCO, the requirements of the STE LCO shall be followed. This includes the SRs specified in the STE LCO.

Some of the STE LCOs require that one or more of the LCOs for normal operation be met (i.e., meeting the STE LCO requires meeting the specified normal LCOs). The Applicability, ACTIONS, and SRs of the specified normal LCOs, however, are not required to be met in order to meet the STE LCO when it is in effect. This means that, upon failure to meet a specified normal LCO, the associated ACTIONS of the STE LCO

BASES

LCO 3.0.7 (continued)

apply, in lieu of the ACTIONS of the normal LCO. Exceptions to the above do exist. There are instances when the Applicability of the specified normal LCO must be met, where its ACTIONS must be taken, where certain of its Surveillances must be performed, or where all of these requirements must be met concurrently with the requirements of the STE LCO.

Unless the SRs of the specified normal LCOs are suspended or changed by the special test, those SRs that are necessary to meet the specified normal LCOs must be met prior to performing the special test. During the conduct of the special test, those Surveillances need not be performed unless specified by the ACTIONS or SRs of the STE LCO.

ACTIONS for STE LCOs provide appropriate remedial measures upon failure to meet the STE LCO. Upon failure to meet these ACTIONS, suspend the performance of the special test and enter the ACTIONS for all LCOs that are then not met. Entry into LCO 3.0.3 may possibly be required, but this determination should not be made by considering only the failure to meet the ACTIONS of the STE LCO.

LCO 3.0.8

LCO 3.0.8 establishes conditions under which systems are considered to remain capable of performing their intended safety function when associated snubbers are not capable of providing their associated support function(s). This LCO states that the supported system is not considered to be inoperable solely due to one or more snubbers not capable of performing their associated support function(s). This is appropriate because a limited length of time is allowed for maintenance, testing, or repair of one or more snubbers not capable of performing their associated support function(s) and appropriate compensatory measures are specified in the snubber requirements, which are located outside of the Technical Specifications (TS) under licensee control. The snubber requirements do not meet the criteria in 10 CFR 50.36(c)(2)(ii), and, as such, are appropriate for control by the licensee.

If the allowed time expires and the snubber(s) are unable to perform their associated support function(s), the affected supported system's LCO(s) must be declared not met and the Conditions and Required Actions entered in accordance with LCO 3.0.2.

LCO 3.0.8.a applies when one or more snubbers are not capable of providing their associated support function(s) to a single train or subsystem of a multiple train or subsystem supported system or to a single train or subsystem supported system. LCO 3.0.8.a allows 72 hours to restore the snubber(s) before declaring the supported system

BASES

LCO 3.0.8 (continued)

inoperable. The 72 hour Completion Time is reasonable based on the low probability of a seismic event concurrent with an event that would require operation of the supported system occurring while the snubber(s) are not capable of performing their associated support function and due to the availability of the redundant train of the supported system.

LCO 3.0.8.b applies when one or more snubbers are not capable of providing their associated support function(s) to more than one train or subsystem of a multiple train or subsystem supported system.
LCO 3.0.8.b allows 12 hours to restore the snubber(s) before declaring the supported system inoperable. The 12 hour Completion Time is reasonable based on the low probability of a seismic event concurrent with an event that would require operation of the supported system occurring while the snubber(s) are not capable of performing their associated support function.

LCO 3.0.8 requires that risk be assessed and managed. Industry and NRC guidance on the implementation of 10 CFR 50.65(a)(4) (the Maintenance Rule) does not address seismic risk. However, use of LCO 3.0.8 should be considered with respect to other plant maintenance activities, and integrated into the existing Maintenance Rule process to the extent possible so that maintenance on any unaffected train or subsystem is properly controlled, and emergent issues are properly addressed. The risk assessment need not be quantified, but may be a qualitative awareness of the vulnerability of systems and components when one or more snubbers are not able to perform their associated support function.

B 3.0 SURVEILLANCE REQUIREMENT (SR) APPLICABILITY

BASES

SRs

SR 3.0.1 through SR 3.0.4 establish the general requirements applicable to all Specifications and apply at all times, unless otherwise stated.

SR 3.0.1

SR 3.0.1 establishes the requirement that SRs must be met during the MODES or other specified conditions in the Applicability for which the requirements of the LCO apply, unless otherwise specified in the individual SRs. This Specification is to ensure that Surveillances are performed to verify the OPERABILITY of systems and components, and that variables are within specified limits. Failure to meet a Surveillance within the specified Frequency, in accordance with SR 3.0.2, constitutes a failure to meet an LCO. Surveillances may be performed by means of any series of sequential, overlapping, or total steps provided the entire Surveillance is performed within the specified Frequency. Additionally, the definitions related to instrument testing (e.g., CHANNEL CALIBRATION) specify that these tests are performed by means of any series of sequential, overlapping, or total steps.

Systems and components are assumed to be OPERABLE when the associated SRs have been met. Nothing in this Specification, however, is to be construed as implying that systems or components are OPERABLE when either:

a. The systems or components are known to be inoperable, although still meeting the SRs or

b. The requirements of the Surveillance(s) are known to be not met between required Surveillance performances.

Surveillances do not have to be performed when the unit is in a MODE or other specified condition for which the requirements of the associated LCO are not applicable, unless otherwise specified. The SRs associated with a special test exception (STE) are only applicable when the STE is used as an allowable exception to the requirements of a Specification.

Unplanned events may satisfy the requirements (including applicable acceptance criteria) for a given SR. In this case, the unplanned event may be credited as fulfilling the performance of the SR. This allowance includes those SRs whose performance is normally precluded in a given MODE or other specified condition.

Surveillances, including Surveillances invoked by Required Actions, do not have to be performed on inoperable equipment because the ACTIONS define the remedial measures that apply. Surveillances have to be met and performed in accordance with SR 3.0.2, prior to returning equipment to OPERABLE status.

BASES

SR 3.0.1 (continued)

Upon completion of maintenance, appropriate post maintenance testing is required to declare equipment OPERABLE. This includes ensuring applicable Surveillances are not failed and their most recent performance is in accordance with SR 3.0.2. Post maintenance testing may not be possible in the current MODE or other specified conditions in the Applicability due to the necessary unit parameters not having been established. In these situations, the equipment may be considered OPERABLE provided testing has been satisfactorily completed to the extent possible and the equipment is not otherwise believed to be incapable of performing its function. This will allow operation to proceed to a MODE or other specified condition where other necessary post maintenance tests can be completed.

Some examples of this process are:

a. Auxiliary feedwater (AFW) pump turbine maintenance during refueling that requires testing at steam pressures > 800 psi. However, if other appropriate testing is satisfactorily completed, the AFW System can be considered OPERABLE. This allows startup and other necessary testing to proceed until the plant reaches the steam pressure required to perform the testing.

b. High pressure safety injection (HPSI) maintenance during shutdown that requires system functional tests at a specified pressure. Provided other appropriate testing is satisfactorily completed, startup can proceed with HPSI considered OPERABLE. This allows operation to reach the specified pressure to complete the necessary post maintenance testing.

SR 3.0.2

SR 3.0.2 establishes the requirements for meeting the specified Frequency for Surveillances and any Required Action with a Completion Time that requires the periodic performance of the Required Action on a "once per..." interval.

SR 3.0.2 permits a 25% extension of the interval specified in the Frequency. This extension facilitates Surveillance scheduling and considers plant operating conditions that may not be suitable for conducting the Surveillance (e.g., transient conditions or other ongoing Surveillance or maintenance activities).

BASES

SR 3.0.2 (continued)

The 25% extension does not significantly degrade the reliability that results from performing the Surveillance at its specified Frequency. This is based on the recognition that the most probable result of any particular Surveillance being performed is the verification of conformance with the SRs. The exceptions to SR 3.0.2 are those Surveillances for which the 25% extension of the interval specified in the Frequency does not apply. These exceptions are stated in the individual Specifications. The requirements of regulations take precedence over the TS. An example of where SR 3.0.2 does not apply is in the Containment Leakage Rate Testing Program. This program establishes testing requirements and Frequencies in accordance with the requirements of regulations. The TS cannot in and of themselves extend a test interval specified in the regulations.

As stated in SR 3.0.2, the 25% extension also does not apply to the initial portion of a periodic Completion Time that requires performance on a "once per ..." basis. The 25% extension applies to each performance after the initial performance. The initial performance of the Required Action, whether it is a particular Surveillance or some other remedial action, is considered a single action with a single Completion Time. One reason for not allowing the 25% extension to this Completion Time is that such an action usually verifies that no loss of function has occurred by checking the status of redundant or diverse components or accomplishes the function of the inoperable equipment in an alternative manner.

The provisions of SR 3.0.2 are not intended to be used repeatedly merely as an operational convenience to extend Surveillance intervals (other than those consistent with refueling intervals) or periodic Completion Time intervals beyond those specified.

SR 3.0.3

SR 3.0.3 establishes the flexibility to defer declaring affected equipment inoperable or an affected variable outside the specified limits when a Surveillance has not been completed within the specified Frequency. A delay period of up to 24 hours or up to the limit of the specified Frequency, whichever is greater, applies from the point in time that it is discovered that the Surveillance has not been performed in accordance with SR 3.0.2, and not at the time that the specified Frequency was not met.

This delay period provides adequate time to complete Surveillances that have been missed. This delay period permits the completion of a Surveillance before complying with Required Actions or other remedial measures that might preclude completion of the Surveillance.

BASES

SR 3.0.3 (continued)

The basis for this delay period includes consideration of unit conditions, adequate planning, availability of personnel, the time required to perform the Surveillance, the safety significance of the delay in completing the required Surveillance, and the recognition that the most probable result of any particular Surveillance being performed is the verification of conformance with the requirements.

When a Surveillance with a Frequency based not on time intervals, but upon specified unit conditions, operating situations, or requirements of regulations (e.g., prior to entering MODE 1 after each fuel loading, or in accordance with 10 CFR 50, Appendix J, as modified by approved exemptions, etc.) is discovered to not have been performed when specified, SR 3.0.3 allows for the full delay period of up to the specified Frequency to perform the Surveillance. However, since there is not a time interval specified, the missed Surveillance should be performed at the first reasonable opportunity.

SR 3.0.3 provides a time limit for, and allowances for the performance of, Surveillances that become applicable as a consequence of MODE changes imposed by Required Actions.

Failure to comply with specified Frequencies for SRs is expected to be an infrequent occurrence. Use of the delay period established by SR 3.0.3 is a flexibility which is not intended to be used as an operational convenience to extend Surveillance intervals. While up to 24 hours or the limit of the specified Frequency is provided to perform the missed Surveillance, it is expected that the missed Surveillance will be performed at the first reasonable opportunity. The determination of the first reasonable opportunity should include consideration of the impact on plant risk (from delaying the Surveillance as well as any plant configuration changes required or shutting the plant down to perform the Surveillance) and impact on any analysis assumptions, in addition to unit conditions, planning, availability of personnel, and the time required to perform the Surveillance. This risk impact should be managed through the program in place to implement 10 CFR 50.65(a)(4) and its implementation guidance, NRC Regulatory Guide 1.182, “Assessing and Managing Risk Before Maintenance Activities at Nuclear Power Plants.” This Regulatory Guide addresses consideration of temporary and aggregate risk impacts, determination of risk management action thresholds, and risk management action up to and including plant

BASES

SR 3.0.3 (continued)

shutdown. The missed Surveillance should be treated as an emergent condition as discussed in the Regulatory Guide. The risk evaluation may use quantitative, qualitative, or blended methods. The degree of depth and rigor of the evaluation should be commensurate with the importance of the component. Missed Surveillances for important components should be analyzed quantitatively. If the results of the risk evaluation determine the risk increase is significant, this evaluation should be used to determine the safest course of action. All missed Surveillances will be placed in the licensee's Corrective Action Program.

If a Surveillance is not completed within the allowed delay period, then the equipment is considered inoperable or the variable is considered outside the specified limits and the Completion Times of the Required Actions for the applicable LCO Conditions begin immediately upon expiration of the delay period. If a Surveillance is failed within the delay period, then the equipment is inoperable, or the variable is outside the specified limits and the Completion Times of the Required Actions for the applicable LCO Conditions begin immediately upon the failure of the Surveillance.

Completion of the Surveillance within the delay period allowed by this Specification, or within the Completion Time of the ACTIONS, restores compliance with SR 3.0.1.

SR 3.0.4

SR 3.0.4 establishes the requirement that all applicable SRs must be met before entry into a MODE or other specified condition in the Applicability.

This Specification ensures that system and component OPERABILITY requirements and variable limits are met before entry into MODES or other specified conditions in the Applicability for which these systems and components ensure safe operation of the unit. The provisions of this Specification should not be interpreted as endorsing the failure to exercise the good practice of restoring systems or components to OPERABLE status before entering an associated MODE or other specified condition in the Applicability.

A provision is included to allow entry into a MODE or other specified condition in the Applicability when an LCO is not met due to a Surveillance not being met in accordance with LCO 3.0.4.

BASES

SR 3.0.4 (continued)

However, in certain circumstances, failing to meet an SR will not result in SR 3.0.4 restricting a MODE change or other specified condition change. When a system, subsystem, division, component, device, or variable is inoperable or outside its specified limits, the associated SR(s) are not required to be performed, per SR 3.0.1, which states that surveillances do not have to be performed on inoperable equipment. When equipment is inoperable, SR 3.0.4 does not apply to the associated SR(s) since the requirement for the SR(s) to be performed is removed. Therefore, failing to perform the Surveillance(s) within the specified Frequency does not result in an SR 3.0.4 restriction to changing MODES or other specified conditions of the Applicability. However, since the LCO is not met in this instance, LCO 3.0.4 will govern any restrictions that may (or may not) apply to MODE or other specified condition changes. SR 3.0.4 does not restrict changing MODES or other specified conditions of the Applicability when a Surveillance has not been performed within the specified Frequency, provided the requirement to declare the LCO not met has been delayed in accordance with SR 3.0.3.

The provisions of SR 3.0.4 shall not prevent entry into MODES or other specified conditions in the Applicability that are required to comply with ACTIONS. In addition, the provisions of SR 3.0.4 shall not prevent changes in MODES or other specified conditions in the Applicability that result from any unit shutdown. In this context, a unit shutdown is defined as a change in MODE or other specified condition in the Applicability associated with transitioning from MODE 1 to MODE 2, MODE 2 to MODE 3, MODE 3 to MODE 4, and MODE 4 to MODE 5.

The precise requirements for performance of SRs are specified such that exceptions to SR 3.0.4 are not necessary. The specific time frames and conditions necessary for meeting the SRs are specified in the Frequency, in the Surveillance, or both. This allows performance of Surveillances when the prerequisite condition(s) specified in a Surveillance procedure require entry into the MODE or other specified condition in the Applicability of the associated LCO prior to the performance or completion of a Surveillance. A Surveillance that could not be performed until after entering the LCO's Applicability, would have its Frequency specified such that it is not "due" until the specific conditions needed are met. Alternately, the Surveillance may be stated in the form of a Note, as not required (to be met or performed) until a particular event, condition, or time has been reached. Further discussion of the specific formats of SRs' annotation is found in Section 1.4, Frequency.

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.1 SHUTDOWN MARGIN (SDM) (Analog)

BASES

BACKGROUND

The reactivity control systems must be redundant and capable of holding the reactor core subcritical when shut down under cold conditions, in accordance with GDC 26 (Ref. 1). Maintenance of the SHUTDOWN MARGIN (SDM) ensures that postulated reactivity events will not damage the fuel. SDM requirements provide sufficient reactivity margin to ensure that acceptable fuel design limits will not be exceeded for normal shutdown and anticipated operational occurrences (AOOs). As such, the SDM defines the degree of subcriticality that would be obtained immediately following the insertion of all control element assemblies (CEAs), assuming the single CEA of highest reactivity worth is fully withdrawn.

The system design requires that two independent reactivity control systems be provided, and that one of these systems be capable of maintaining the core subcritical under cold conditions. These requirements are provided by the use of movable CEAs and soluble boric acid in the Reactor Coolant System (RCS). The CEA System provides the SDM during power operation and is capable of making the core subcritical rapidly enough to prevent exceeding acceptable fuel damage limits, assuming that the CEA of highest reactivity worth remains fully withdrawn.

The soluble boron system can compensate for fuel depletion during operation and all xenon burnout reactivity changes, and maintain the reactor subcritical under cold conditions.

During power operation, SDM control is ensured by operating with the shutdown CEAs fully withdrawn and the regulating CEAs within the limits of LCO 3.1.6, "Regulating Control Element Assembly (CEA) Insertion Limits." When the unit is in the shutdown and refueling modes, the SDM requirements are met by means of adjustments to the RCS boron concentration.

APPLICABLE SAFETY ANALYSES

The minimum required SDM is assumed as an initial condition in safety analysis. The safety analysis (Ref. 2) establishes an SDM that ensures specified acceptable fuel design limits are not exceeded for normal operation and AOOs, with the assumption of the highest worth CEA stuck out following a reactor trip. For MODE 5, the primary safety analysis that relies on the SDM limits is the boron dilution analysis.

BASES

APPLICABLE SAFETY ANALYSES (continued)

The acceptance criteria for the SDM requirements are that specified acceptable fuel design limits are maintained. This is done by ensuring that:

a. The reactor can be made subcritical from all operating conditions, transients, and Design Basis Events,

b. The reactivity transients associated with postulated accident conditions are controllable within acceptable limits (departure from nucleate boiling ratio (DNBR), fuel centerline temperature limit AOOs, and ≤ 280 cal/gm energy deposition for the CEA ejection accident), and

c. The reactor will be maintained sufficiently subcritical to preclude inadvertent criticality in the shutdown condition.

The most limiting accident for the SDM requirements are based on a main steam line break (MSLB), as described in the accident analysis (Ref. 2). The increased steam flow resulting from a pipe break in the main steam system causes an increased energy removal from the affected steam generator (SG), and consequently the RCS. This results in a reduction of the reactor coolant temperature. The resultant coolant shrinkage causes a reduction in pressure. In the presence of a negative moderator temperature coefficient, this cooldown causes an increase in core reactivity. As RCS temperature decreases, the severity of an MSLB decreases until the MODE 5 value is reached. The most limiting MSLB, with respect to potential fuel damage before a reactor trip occurs, is a guillotine break of a main steam line inside containment initiated at the end of core life. The positive reactivity addition from the moderator temperature decrease will terminate when the affected SG boils dry, thus terminating RCS heat removal and cooldown. Following the MSLB, a post trip return to power may occur; however, no fuel damage occurs as a result of the post trip return to power, and THERMAL POWER does not violate the Safety Limit (SL) requirement of SL 2.1.1.

In addition to the limiting MSLB transient, the SDM requirement for MODES 3 and 4 must also protect against:

BASES

APPLICABLE SAFETY ANALYSES (continued)

a. Inadvertent boron dilution,

b. An uncontrolled CEA withdrawal from a subcritical condition,

c. Startup of an inactive reactor coolant pump (RCP), and

d. CEA ejection.

Each of these events is discussed below.

In the boron dilution analysis, the required SDM defines the reactivity difference between an initial subcritical boron concentration and the corresponding critical boron concentration. These values, in conjunction with the configuration of the RCS and the assumed dilution flow rate, directly affect the results of the analysis. This event is most limiting at the beginning of core life when critical boron concentrations are highest.

The withdrawal of CEAs from subcritical conditions adds reactivity to the reactor core, causing both the core power level and heat flux to increase with corresponding increases in reactor coolant temperatures and pressure. The withdrawal of CEAs also produces a time dependent redistribution of core power.

Depending on the system initial conditions and reactivity insertion rate, the uncontrolled CEA withdrawal transient is terminated by either a high power trip or a high pressurizer pressure trip. In all cases, power level, RCS pressure, linear heat rate, and the DNBR do not exceed allowable limits.

The startup of an inactive RCP will not result in a "cold water" criticality, even if the maximum difference in temperature exists between the SG and the core. The maximum positive reactivity addition that can occur due to an inadvertent RCP start is less than half the minimum required SDM. An idle RCP cannot, therefore, produce a return to power from the hot standby condition.

SDM satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO

The MSLB (Ref. 2) and the boron dilution (Ref. 3) accidents are the most limiting analyses that establish the SDM value of the LCO. For MSLB accidents, if the LCO is violated, there is a potential to exceed the DNBR limit and to exceed 10 CFR 100, "Reactor Site Criteria," limits (Ref. 4). For the boron dilution accident, if the LCO is violated, then the minimum required time assumed for operator action to terminate dilution may no longer be applicable.

SDM is a core physics design condition that can be ensured through CEA positioning (regulating and shutdown CEA) and through the soluble boron concentration.

APPLICABILITY

In MODES 3, 4, and 5, the SDM requirements are applicable to provide sufficient negative reactivity to meet the assumptions of the safety analyses discussed above. In MODES 1 and 2, SDM is ensured by complying with LCO 3.1.5, "Shutdown Control Element Assembly (CEA) Insertion Limits," and LCO 3.1.6. In MODE 6, the shutdown reactivity requirements are given in LCO 3.9.1, "Boron Concentration."

ACTIONS

A.1

If the SDM requirements are not met, boration must be initiated promptly. A Completion Time of 15 minutes is adequate for an operator to correctly align and start the required systems and components. It is assumed that boration will be continued until the SDM requirements are met.

In the determination of the required combination of boration flow rate and boron concentration, there is no unique requirement that must be satisfied. Since it is imperative to raise the boron concentration of the RCS as soon as possible, the boron concentration should be a highly concentrated solution, such as that normally found in the boric acid storage tank or the borated water storage tank. The operator should borate with the best source available for the plant conditions.

In determining the boration flow rate, the time core life must be considered. For instance, the most difficult time in core life to increase the RCS boron concentration is at the beginning of cycle, when the boron concentration may approach or exceed 2000 ppm. Assuming that a value of 1% $\Delta k/k$ must be recovered and a boration flow rate of [ ] gpm, it is possible to increase the boron concentration of the RCS by 100 ppm in approximately 35 minutes. If a boron worth of 10 pcm/ppm is assumed, this combination of parameters will increase the SDM by 1% $\Delta k/k$. These boration parameters of [ ] gpm and [ ] ppm represent typical values and are provided for the purpose of offering a specific example.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.1.1.1

SDM is verified by performing a reactivity balance calculation, considering the listed reactivity effects:

a. RCS boron concentration,

b. CEA positions,

c. RCS average temperature,

d. Fuel burnup based on gross thermal energy generation,

e. Xenon concentration,

f. Samarium concentration, and

g. Isothermal temperature coefficient (ITC).

Using the ITC accounts for Doppler reactivity in this calculation because the reactor is subcritical and the fuel temperature will be changing at the same rate as the RCS.

The Frequency of 24 hours is based on the generally slow change in required boron concentration, and also allows sufficient time for the operator to collect the required data, which includes performing a boron concentration analysis, and complete the calculation.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 26.

2. FSAR, Section [ ].

3. FSAR, Section [ ].

4. 10 CFR 100.

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.2 Reactivity Balance (Analog)

BASES

BACKGROUND

According to GDC 26, GDC 28, and GDC 29 (Ref. 1), reactivity shall be controllable, such that, subcriticality is maintained under cold conditions, and acceptable fuel design limits are not exceeded during normal operation and anticipated operational occurrences. Therefore, reactivity balance is used as a measure of the predicted versus measured core reactivity during power operation. The periodic confirmation of core reactivity is necessary to ensure that Design Basis Accident (DBA) and transient safety analyses remain valid. A large reactivity difference could be the result of unanticipated changes in fuel, control element assembly (CEA) worth, or operation at conditions not consistent with those assumed in the predictions of core reactivity, and could potentially result in a loss of SDM or violation of acceptable fuel design limits. Comparing predicted versus measured core reactivity validates the nuclear methods used in the safety analysis and supports the SDM demonstrations (LCO 3.1.1, "SHUTDOWN MARGIN (SDM)") in ensuring the reactor can be brought safely to cold, subcritical conditions.

When the reactor core is critical or in normal power operation, a reactivity balance exists and the net reactivity is zero. A comparison of predicted and measured reactivity is convenient under such a balance, since parameters are being maintained relatively stable under steady state power conditions. The positive reactivity inherent in the core design is balanced by the negative reactivity of the control components, thermal feedback, neutron leakage, and materials in the core that absorb neutrons, such as burnable absorbers producing zero net reactivity. Excess reactivity can be inferred from the critical boron curve, which provides an indication of the soluble boron concentration in the Reactor Coolant System (RCS) versus cycle burnup. Periodic measurement of the RCS boron concentration for comparison with the predicted value with other variables fixed (such as CEA height, temperature, pressure, and power) provides a convenient method of ensuring that core reactivity is within design expectations, and that the calculational models used to generate the safety analysis are adequate.

In order to achieve the required fuel cycle energy output, the uranium enrichment in the new fuel loading and in the fuel remaining from the previous cycle, provides excess positive reactivity beyond that required to sustain steady state operation throughout the cycle. When the reactor is critical at RTP and moderator temperature, the excess positive reactivity is compensated by burnable absorbers (if any), CEAs, whatever neutron poisons (mainly xenon and samarium) are present in the fuel, and the RCS boron concentration.

BASES

BACKGROUND (continued)

When the core is producing THERMAL POWER, the fuel is being depleted and excess reactivity is decreasing. As the fuel depletes, the RCS boron concentration is reduced to decrease negative reactivity and maintain constant THERMAL POWER. The critical boron curve is based on steady state operation at RTP. Therefore, deviations from the predicted critical boron curve may indicate deficiencies in the design analysis, deficiencies in the calculational models, or abnormal core conditions, and must be evaluated.

APPLICABLE SAFETY ANALYSES

Accurate prediction of core reactivity is either an explicit or implicit assumption in the accident analysis evaluations. Every accident evaluation (Ref. 2) is, therefore, dependent upon accurate evaluation of core reactivity. In particular, SDM and reactivity transients, such as CEA withdrawal accidents or CEA ejection accidents, are very sensitive to accurate prediction of core reactivity. These accident analysis evaluations rely on computer codes that have been qualified against available test data, operating plant data, and analytical benchmarks. Monitoring reactivity balance additionally ensures that the nuclear methods provide an accurate representation of the core reactivity.

Design calculations and safety analyses are performed for each fuel cycle for the purpose of predetermining reactivity behavior and the RCS boron concentration requirements for reactivity control during fuel depletion.

The comparison between measured and predicted initial core reactivity provides a normalization for calculational models used to predict core reactivity. If the measured and predicted RCS boron concentrations for identical core conditions at beginning of cycle (BOC) do not agree, then the assumptions used in the reload cycle design analysis or the calculational models used to predict soluble boron requirements may not be accurate. If reasonable agreement between measured and predicted core reactivity exists at BOC, then the prediction may be normalized to the measured boron concentration. Thereafter, any significant deviations in the measured boron concentration from the predicted critical boron curve that develop during fuel depletion may be an indication that the calculational model is not adequate for core burnups beyond BOC, or that an unexpected change in core conditions has occurred.

BASES

APPLICABLE SAFETY ANALYSES (continued)

The normalization of predicted RCS boron concentration to the measured value is typically performed after reaching RTP following startup from a refueling outage, with the CEAs in their normal positions for power operation. The normalization is performed at BOC conditions, so that core reactivity relative to predicted values can be continually monitored and evaluated as core conditions change during the cycle.

The reactivity balance satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

The reactivity balance limit is established to ensure plant operation is maintained within the assumptions of the safety analyses. Large differences between actual and predicted core reactivity may indicate that the assumptions of the DBA and transient analyses are no longer valid, or that the uncertainties in the nuclear design methodology are larger than expected. A limit on the reactivity balance of ± 1% $\Delta k/k$ has been established, based on engineering judgment. A 1% deviation in reactivity from that predicted is larger than expected for normal operation and should therefore be evaluated.

When measured core reactivity is within 1% $\Delta k/k$ of the predicted value at steady state thermal conditions, the core is considered to be operating within acceptable design limits. Since deviations from the limit are normally detected by comparing predicted and measured steady state RCS critical boron concentrations, the difference between measured and predicted values would be approximately 100 ppm (depending on the boron worth) before the limit is reached. These values are well within the uncertainty limits for analysis of boron concentration samples, so that spurious violations of the limit due to uncertainty in measuring the RCS boron concentration are unlikely.

APPLICABILITY

The limits on core reactivity must be maintained during MODES 1 and 2 because a reactivity balance must exist when the reactor is critical or producing THERMAL POWER. As the fuel depletes, core conditions are changing, and confirmation of the reactivity balance ensures the core is operating as designed. This Specification does not apply in MODES 3, 4, and 5 because the reactor is shut down and the reactivity balance is not changing.

In MODE 6, fuel loading results in a continually changing core reactivity. Boron concentration requirements (LCO 3.9.1, "Boron Concentration") ensure that fuel movements are performed within the bounds of the safety analysis. An SDM demonstration is required during the first startup following operations that could have altered core reactivity (e.g., fuel movement, or CEA replacement, or shuffling).

BASES

ACTIONS

A.1 and A.2

Should an anomaly develop between measured and predicted core reactivity, an evaluation of the core design and safety analysis must be performed. Core conditions are evaluated to determine their consistency with input to design calculations. Measured core and process parameters are evaluated to determine that they are within the bounds of the safety analysis, and safety analysis calculational models are reviewed to verify that they are adequate for representation of the core conditions. The required Completion Time of 7 days is based on the low probability of a DBA occurring during this period, and allows sufficient time to assess the physical condition of the reactor and complete the evaluation of the core design and safety analysis.

Following evaluations of the core design and safety analysis, the cause of the reactivity anomaly may be resolved. If the cause of the reactivity anomaly is a mismatch in core conditions at the time of RCS boron concentration sampling, then a recalculation of the RCS boron concentration requirements may be performed to demonstrate that core reactivity is behaving as expected. If an unexpected physical change in the condition of the core has occurred, it must be evaluated and corrected, if possible. If the cause of the reactivity anomaly is in the calculation technique, then the calculational models must be revised to provide more accurate predictions. If any of these results are demonstrated, and it is concluded that the reactor core is acceptable for continued operation, then the boron letdown curve may be renormalized, and power operation may continue. If operational restrictions or additional SRs are necessary to ensure the reactor core is acceptable for continued operation, then they must be defined.

The required Completion Time of 7 days is adequate for preparing whatever operating restrictions or Surveillances that may be required to allow continued reactor operation.

B.1

If the core reactivity cannot be restored to within the 1% $\Delta k/k$ limit, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours. If the SDM for MODE 3 is not met, then boration required by SR 3.1.1.1 would occur. The allowed Completion Time is reasonable, based on operating experience, for reaching MODE 3 from full power conditions in an orderly manner and without challenging plant systems.

BASES

SURVEILLANCE REQUIREMENTS	SR 3.1.2.1 Core reactivity is verified by periodic comparisons of measured and predicted RCS boron concentrations. The comparison is made considering that other core conditions are fixed or stable including CEA position, moderator temperature, fuel temperature, fuel depletion, xenon concentration, and samarium concentration. The Surveillance is performed prior to entering MODE 1 as an initial check on core conditions and design calculations at BOC. The SR is modified by three Notes. Note 1 in the Surveillance column indicates that the normalization of predicted core reactivity to the measured value must take place within the first 60 effective full power days (EFPD) after each fuel loading. This allows sufficient time for core conditions to reach steady state, but prevents operation for a large fraction of the fuel cycle without establishing a benchmark for the design calculations. The required subsequent Frequency of 31 EFPD following the initial 60 EFPD after entering MODE 1, is acceptable, based on the slow rate of core changes due to fuel depletion and the presence of other indicators (e.g., QPTR, etc.) for prompt indication of an anomaly. A second Note, "only required after 60 EFPD," is added to the Frequency column to allow this. Note 2 in the Surveillance column indicates that the performance of SR 3.1.2.1 is not required prior to entering MODE 2. This Note is required to allow a MODE 2 entry to verify core reactivity, because LCO Applicability is for MODES 1 and 2.
REFERENCES	1. 10 CFR 50, Appendix A, GDC 26, GDC 28, and GDC 29. 2. FSAR, Section [ ].

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.3 Moderator Temperature Coefficient (MTC) (Analog)

BASES

BACKGROUND

According to GDC 11 (Ref. 1), the reactor core and its interaction with the Reactor Coolant System (RCS) must be designed for inherently stable power operation, even in the possible event of an accident. In particular, the net reactivity feedback in the system must compensate for any unintended or rapid reactivity increases.

The MTC relates a change in core reactivity to a change in reactor coolant temperature. A positive MTC means that reactivity increases with increasing moderator temperature; conversely, a negative MTC means that reactivity decreases with increasing moderator temperature. The reactor is designed to operate with a negative MTC over the largest possible range of fuel cycle operation. Therefore, a coolant temperature increase will cause a reactivity decrease, so that the coolant temperature tends to return toward its initial value. Reactivity increases that cause a coolant temperature increase will thus be self limiting, and stable power operation will result. The same characteristic is true when the MTC is positive and coolant temperature decreases occur.

MTC values are predicted at selected burnups during the safety evaluation analysis and are confirmed to be acceptable by measurements. Both initial and reload cores are designed so that the beginning of cycle (BOC) MTC is less positive than that allowed by the LCO. The actual value of the MTC is dependent on core characteristics, such as fuel loading and reactor coolant soluble boron concentration. The core design may require additional fixed distributed poisons (lumped burnable poison assemblies) to yield an MTC at the BOC within the range analyzed in the plant accident analysis. The end of cycle (EOC) MTC is also limited by the requirements of the accident analysis. Fuel cycles that are designed to achieve high burnups or that have changes to other characteristics are evaluated to ensure that the MTC does not exceed the EOC limit.

APPLICABLE SAFETY ANALYSES

The acceptance criteria for the specified MTC are:

a. The MTC values must remain within the bounds of those used in the accident analysis (Ref. 2) and

b. The MTC must be such that inherently stable power operations result during normal operation and during accidents, such as overheating and overcooling events.

BASES

APPLICABLE SAFETY ANALYSES (continued)

Reference 2 contains analyses of accidents that result in both overheating and overcooling of the reactor core. MTC is one of the controlling parameters for core reactivity in these accidents. Both the most positive value and most negative value of the MTC are important to safety, and both values must be bounded. Values used in the analyses consider worst case conditions, such as very large soluble boron concentrations, to ensure the accident results are bounding (Ref. 3).

Accidents that cause core overheating, either by decreased heat removal or increased power production, must be evaluated for results when the MTC is positive. Reactivity accidents that cause increased power production include the control element assembly (CEA) withdrawal transient from either zero or full THERMAL POWER. The limiting overheating event relative to plant response is based on the maximum difference between core power and steam generator heat removal during a transient. The most limiting event with respect to a positive MTC is a CEA withdrawal accident from zero power, also referred to as a startup accident (Ref. 4).

Accidents that cause core overcooling must be evaluated for results when the MTC is most negative. The event that produces the most rapid cooldown of the RCS, and is therefore the most limiting event with respect to the negative MTC, is a steam line break (SLB) event. Following the reactor trip for the postulated EOC SLB event, the large moderator temperature reduction combined with the large negative MTC may produce reactivity increases that are as much as the shutdown reactivity. When this occurs, a substantial fraction of core power is produced with all CEAs inserted, except the most reactive one, which is assumed withdrawn. Even if the reactivity increase produces slightly subcritical conditions, a large fraction of core power may be produced through the effects of subcritical neutron multiplication.

MTC values are bounded in reload safety evaluations assuming steady state conditions at BOC and EOC. A middle of cycle (MOC) measurement is conducted at conditions when the RCS boron concentration reaches approximately 300 ppm. The measured value may be extrapolated to project the EOC value, in order to confirm reload design predictions.

The MTC satisfies Criterion 2 of the NRC Policy Statement.

BASES

LCO

LCO 3.1.3 requires the MTC to be within specified limits of the COLR to ensure the core operates within the assumptions of the accident analysis. During the reload core safety evaluation, the MTC is analyzed to determine that its values remain within the bounds of the original accident analysis during operation. The limit on a positive MTC ensures that core overheating accidents will not violate the accident analysis assumptions. The negative MTC limit for EOC specified in the COLR ensures that core overcooling accidents will not violate the accident analysis assumptions.

MTC is a core physics parameter determined by the fuel and fuel cycle design and cannot be easily controlled once the core design is fixed. During operation, therefore, the LCO can only be ensured through measurement. The surveillance checks at BOC and MOC on an MTC provide confirmation that the MTC is behaving as anticipated, so that the acceptance criteria are met.

APPLICABILITY

In MODE 1, the limits on the MTC must be maintained to ensure that any accident initiated from THERMAL POWER operation will not violate the design assumptions of the accident analysis. In MODE 2, the limits must also be maintained to ensure startup and subcritical accidents, such as the uncontrolled CEA or group withdrawal, will not violate the assumptions of the accident analysis. In MODES 3, 4, 5, and 6, this LCO is not applicable, since no Design Basis Accidents (DBAs) using the MTC as an analysis assumption are initiated from these MODES. However, the variation of the MTC, with temperature in MODES 3, 4, and 5, for DBAs initiated in MODES 1 and 2, is accounted for in the subject accident analysis. The variation of the MTC, with temperature assumed in the safety analysis, is accepted as valid once the BOC and MOC measurements are used for normalization.

ACTIONS

A.1

MTC is a function of the fuel and fuel cycle designs, and cannot be controlled directly once the designs have been implemented in the core. If MTC exceeds its limits, the reactor must be placed in MODE 3. This eliminates the potential for violation of the accident analysis bounds. The associated Completion Time of 6 hours is reasonable, considering the probability of an accident occurring during the time period that would require an MTC value within the LCO limits, and the time for reaching MODE 3 from full power conditions in an orderly manner and without challenging plant systems.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.1.3.1 and SR 3.1.3.2

The SRs for measurement of the MTC at the beginning and middle of each fuel cycle provide for confirmation of the limiting MTC values. The MTC changes smoothly from most positive (least negative) to most negative value during fuel cycle operation, as the RCS boron concentration is reduced to compensate for fuel depletion. The requirement for measurement prior to operation > 5% RTP satisfies the confirmatory check on the most positive (least negative) MTC value. The requirement for measurement, within 7 days after reaching 40 effective full power days and b core burnup, satisfies the confirmatory check of the most negative MTC value. The measurement is performed at any THERMAL POWER, so that the projected EOC MTC may be evaluated before the reactor actually reaches the EOC condition. MTC values may be extrapolated and compensated to permit direct comparison to the specified MTC limits.

SR 3.1.3.2 is modified by a Note, which indicates that if the extrapolated MTC is more negative than the EOC COLR limit, the Surveillance may be repeated, and that shutdown must occur prior to exceeding the minimum allowable boron concentration at which MTC is projected to exceed the lower limit. An engineering evaluation is performed if the extrapolated value of MTC exceeds the Specification limits.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 11.

2. FSAR, Section [ ].

3. FSAR, Section [ ].

4. FSAR, Section [ ].

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.4 Control Element Assembly (CEA) Alignment (Analog)

BASES

BACKGROUND

The OPERABILITY (i.e., trippability) of the shutdown and regulating Control Element Assemblies (CEAs) is an initial assumption in all safety analyses that assume CEA insertion upon reactor trip. Maximum CEA misalignment is an initial assumption in the safety analysis that directly affects core power distributions and assumptions of available SDM.

The applicable criteria for these reactivity and power distribution design requirements are 10 CFR 50, Appendix A, GDC 10 and GDC 26 (Ref. 1), and 10 CFR 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Nuclear Power Plants" (Ref. 2).

Mechanical or electrical failures may cause a CEA to become inoperable or to become misaligned from its group. CEA inoperability or misalignment may cause increased power peaking, due to the asymmetric reactivity distribution and a reduction in the total available CEA worth for reactor shutdown. Therefore, CEA alignment and OPERABILITY are related to core operation in design power peaking limits and the core design requirement of a minimum SDM.

Limits on CEA alignment and OPERABILITY have been established, and all CEA positions are monitored and controlled during power operation to ensure that the power distribution and reactivity limits defined by the design power peaking and SDM limits are preserved.

CEAs are moved by their control element drive mechanisms (CEDMs). Each CEDM moves its CEA one step (approximately ¾ inch) at a time, but at varying rates (steps per minute) depending on the signal output from the Control Element Drive Mechanism Control System (CEDMCS).

The CEAs are arranged into groups that are radially symmetric. Therefore, movement of the CEAs does not introduce radial asymmetries in the core power distribution. The shutdown and regulating CEAs provide the required reactivity worth for immediate reactor shutdown upon a reactor trip. The regulating CEAs also provide reactivity (power level) control during normal operation and transients. Their movement may be automatically controlled by the Reactor Regulating System.

The axial position of shutdown and regulating CEAs is indicated by two separate and independent systems, which are the Plant Computer CEA Position Indication System and the Reed Switch Position Indication System.

BASES

BACKGROUND (continued)

The Plant Computer CEA Position Indication System counts the commands sent to the CEA gripper coils from the CEDM Control System that moves the CEAs. There is a one step counter for each group of CEAs. Individual CEAs in a group all receive the same signal to move and should, therefore, all be at the same position indicated by the group step counter for that group. Plant Computer CEA Position Indication System is considered highly precise (± 1 step or ± ¾ inch). If a CEA does not move one step for each command signal, the step counter will still count the command and incorrectly reflect the position of the CEA.

The Reed Switch Position Indication System provides a highly accurate indication of actual CEA position, but at a lower precision than the step counters. This system is based on inductive analog signals from a series of reed switches spaced along a tube with a center to center distance of 1.5 inches, which is two steps. To increase the reliability of the system, there are redundant reed switches at each position.

APPLICABLE SAFETY ANALYSES

CEA misalignment accidents are analyzed in the safety analysis (Ref. 3). The accident analysis defines CEA misoperation as any event, with the exception of sequential group withdraws, which could result from a single malfunction in the reactivity control systems. For example, CEA misalignment may be caused by a malfunction of the CEDM, CEDMCS, or by operator error. A stuck CEA may be caused by mechanical jamming of the CEA fingers or of the gripper. Inadvertent withdrawal of a single CEA may be caused by the opening of the electrical circuit of the CEDM holding coil for a full length or part length CEA. A dropped CEA could be caused by an electrical failure in the CEA coil power programmers.

The acceptance criteria for addressing CEA inoperability or misalignment are that:

a. There shall be no violations of either:

    1. Specified acceptable fuel design limits or

    2. Reactor Coolant System (RCS) pressure boundary integrity and

b. The core must remain subcritical after accident transients.

BASES

APPLICABLE SAFETY ANALYSES (continued)

Three types of misalignment are distinguished in the safety analysis (Ref. 1). During movement of a group, one CEA may stop moving while the other CEAs in the group continue. This condition may cause excessive power peaking. The second type of misalignment occurs if one CEA fails to insert upon a reactor trip and remains stuck fully withdrawn. This condition requires an evaluation to determine that sufficient reactivity worth is held in the remaining CEAs to meet the SDM requirement with the maximum worth CEA stuck fully withdrawn. If a CEA is stuck in the fully withdrawn position, its worth is added to the SDM requirement, since the safety analysis does not take two stuck CEAs into account. The third type of misalignment occurs when one CEA drops partially or fully into the reactor core. This event causes an initial power reduction followed by a return towards the original power, due to positive reactivity feedback from the negative moderator temperature coefficient. Increased peaking during the power increase may result in excessive local linear heat rates (LHRs).

Two types of analyses are performed in regard to static CEA misalignment (Ref. 4). With CEA banks at their insertion limits, one type of analysis considers the case when any one CEA is inserted [ ] inches into the core. The second type of analysis considers the case of a single CEA withdrawn [ ] inches from a bank inserted into its insertion limit. Satisfying limits on departure from nucleate boiling ratio (DNBR) in both of these cases bounds the situation when a CEA is misaligned from its group by [7 inches].

Another type of misalignment occurs if one CEA fails to insert upon a reactor trip and remains stuck fully withdrawn. This condition is assumed in the evaluation to determine that the required SDM is met with the maximum worth CEA also fully withdrawn (Ref. 5).

Since the CEA drop incidents result in the most rapid approach to specified acceptable fuel design limits (SAFDLs) caused by a CEA misoperation, the accident analysis analyzed a single full length CEA drop. The most rapid approach to the DNBR SAFDL may be caused by a single full length CEA drop or a CEA subgroup drop, depending upon initial conditions.

All of the above CEA misoperations will result in an automatic reactor trip. In the case of the full length CEA drop, a prompt decrease in core average power and a distortion in radial power are initially produced, which, when conservatively coupled, result in a local power and heat flux increase, and a decrease in DNBR parameters.

BASES

APPLICABLE SAFETY ANALYSES (continued)

The results of the CEA misoperation analysis show that during the most limiting misoperation events, no violations of the SAFDLs, fuel centerline temperature, or RCS pressure occur.

CEA alignment limits and OPERABILITY requirements satisfy Criteria 2 and 3 of 10 CFR 50.36(c)(2)(ii).

LCO

The limits on shutdown and regulating CEA alignments ensure that the assumptions in the safety analysis will remain valid. The requirements on CEA OPERABILITY ensure that upon reactor trip, the CEAs will be available and will be inserted to provide enough negative reactivity to shut down the reactor. The CEA OPERABILITY requirements (i.e., trippability) are separate from alignment requirements which ensure that the CEA banks maintain the correct power distribution and CEA alignment. The CEA OPERABILITY requirement is satisfied provided the CEA will fully insert in the required CEA drop time assumed in the safety analysis. CEA control malfunctions that result in the inability to move a CEA (e.g., CEA lift rod failures), but do not impact trippability, do not result in CEA inoperability.

The requirement is to maintain the CEA alignment to within [7 inches] between any CEA and its group. The minimum misalignment assumed in safety analysis is [15 inches], and in some cases, a total misalignment from fully withdrawn to fully inserted is assumed.

Failure to meet the requirements of this LCO may produce unacceptable power peaking factors and LHRs, or unacceptable SDMS, all of which may constitute initial conditions inconsistent with the safety analysis.

APPLICABILITY

The requirements on CEA OPERABILITY and alignment are applicable in MODES 1 and 2 because these are the only MODES in which neutron (or fission) power is generated, and the OPERABILITY (i.e., trippability) and alignment of CEAs have the potential to affect the safety of the plant. In MODES 3, 4, 5, and 6, the alignment limits do not apply because the CEAs are bottomed, and the reactor is shut down and not producing fission power. In the shutdown Modes, the OPERABILITY of the shutdown and regulating CEAs has the potential to affect the required SDM, but this effect can be compensated for by an increase in the boron concentration of the RCS. See LCO 3.1.1, "SHUTDOWN MARGIN (SDM)," for SDM in MODES 3, 4, and 5, and LCO 3.9.1, "Boron Concentration," for boron concentration requirements during refueling.

BASES

ACTIONS

A.1 and A.2

If one or more CEAs (regulating or shutdown) are misaligned by > [7 inches] and ≤ [15 inches], or one CEA is misaligned by > [15 inches], continued operation in MODES 1 and 2 may continue, provided, within 1 hour, the power is reduced to ≤ 70% RTP, and within 2 hours CEA alignment is restored. Regulating CEA alignment can be restored by either aligning the misaligned CEA(s) to within [7 inches] of its group or aligning the misaligned CEA's group to within [7 inches] of the misaligned CEA. Shutdown CEA alignment can be restored by aligning the misaligned CEA(s) to within [7 inches] of its group.

Xenon redistribution in the core starts to occur as soon as a CEA becomes misaligned. Reducing THERMAL POWER in accordance with Figure 3.1.4-1 (in the associated LCO) ensures acceptable power distributions are maintained (Ref. 6). For small misalignments (< [15 inches]) of the CEAs, there is:

a. A small effect on the time dependent long term power distributions relative to those used in generating LCOs and limiting safety system settings (LSSS) setpoints,

b. A negligible effect on the available SDM, and

c. A small effect on the ejected CEA worth used in the accident analysis.

With a large CEA misalignment (≥ [15 inches]), however, this misalignment would cause distortion of the core power distribution. This distortion may, in turn, have a significant effect on the time dependent, long term power distributions relative to those used in generating LCOs and LSSS setpoints. The effect on the available SDM and the ejected CEA worth used in the accident analysis remain small. Therefore, this condition is limited to a single CEA misalignment, while still allowing 2 hours for recovery.

In both cases, a 2 hour time period is sufficient to:

a. Identify cause of a misaligned CEA,

b. Take appropriate corrective action to realign the CEAs, and

c. Minimize the effects of xenon redistribution.

BASES

ACTIONS (continued)

If a CEA is untrippable, it is not available for reactivity insertion during a reactor trip. With an untrippable CEA, meeting the insertion limits of LCO 3.1.5 and LCO 3.1.6 does not ensure that adequate SDM exists. The CEA must be returned to OPERABLE status with 2 hours or transition to MODE 3.

B.1, B.2.1, and B.2.2

The CEA motion inhibit permits CEA motion within the requirements of LCO 3.1.6, "Regulating Control Element Assembly Insertion Limits," and prevents regulating CEAs from being misaligned from other CEAs in the group.

Performing SR 3.1.4.1 within 1 hour and every 4 hours thereafter, is considered acceptable in view of other information continuously available to the operator in the control room.

With the CEA motion inhibit inoperable, a Completion Time of 6 hours is allowed for restoring the CEA motion inhibit to OPERABLE status, or placing and maintaining the CEA drive switch in either the "off" or "manual" position, fully withdrawing the CEAs in groups 3 and 4, and withdrawing all CEAs in group 5 to < 5% insertion.

Placing the CEA drive switch in the "off" or "manual" position ensures the CEAs will not move in response to Reactor Regulating System automatic motion commands. Withdrawal of the CEAs to the positions required in the Required Action B.2.2 ensures that core perturbations in local burnup, perking factors, and SDM will not be more adverse than the Conditions assumed in the safety analyses and LCO setpoint determination (Ref. 6).

The 6 hour Completion Time takes into account Required Action B.1, the protection afforded by the CEA deviation circuits, and other information continuously available to the operator in the control room, so that during actual CEA motion, deviations can be detected.

Required Action B.2.2 is modified by a Note indicating that this Required Action shall not be performed when in conflict with either Required Action A.1, A.2, or C.1.

BASES

ACTIONS (continued)

C.1

When the CEA deviation circuit is inoperable, performing SR 3.1.4.1, within 1 hour and every 4 hours thereafter, ensures improper CEA alignments are identified before unacceptable flux distributions occur. The specified Completion Times take into account other information continuously available to the operator in the control room, so that during CEA movement, deviations can be detected, and the protection provided by the CEA inhibit and deviation circuit is not required.

D.1

If the Required Action or associated Completion Time of Condition A, Condition B, or Condition C is not met, one or more regulating or shutdown CEAs are inoperable, or two or more CEAs are misaligned by > [15 inches], the unit is required to be brought to MODE 3. By being brought to MODE 3, the unit is brought outside its MODE of applicability. Continued operation is not allowed in the case of more than one CEA misaligned from any other CEA in its group by > [15 inches], or one or more CEAs inoperable. This is because these cases are indicative of a loss of SDM and power distribution, and a loss of safety function, respectively.

When a Required Action cannot be completed within the required Completion Time, a controlled shutdown should be commenced. The allowed Completion Time of 6 hours is reasonable, based on operating experience, for reaching MODE 3 from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.1.4.1

Verification that individual CEA positions are within [7 inches] (indicated reed switch positions) of all other CEAs in the group at Frequencies of within 1 hour of any CEA movement of > 7.5 inches and every 12 hours. The CEA position verification after each movement of > 7.5 inches ensures that the CEAs in that group are properly aligned at the time when CEA misalignments are most likely to have occurred. The 12 hour Frequency allows the operator to detect a CEA that is beginning to deviate from its expected position. The specified Frequency takes into account other CEA position information that is continuously available to the operator in the control room, so that during CEA movement, deviations can be detected, and protection can be provided by the CEA motion inhibit and deviation circuits.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.1.4.2

Demonstrating the CEA motion inhibit OPERABLE verifies that the CEA motion inhibit is functional, even if it is not regularly operated. The 92 day Frequency takes into account other information continuously available to the operator in the control room, so that during CEA movement, deviations can be detected, and protection can be provided by the CEA deviation circuits.

SR 3.1.4.3

Demonstrating the CEA deviation circuit is OPERABLE verifies the circuit is functional. The 92 day Frequency takes into account other information continuously available to the operator in the control room, so that during CEA movement, deviations can be detected, and protection can be provided by the CEA motion inhibit.

SR 3.1.4.4

Verifying each CEA is trippable would require that each CEA be tripped. In MODES 1 and 2, tripping each CEA would result in radial or axial power tilts, or oscillations. Therefore, individual CEAs are exercised every 92 days to provide increased confidence that all CEAs continue to be trippable, even if they are not regularly tripped. A movement of [5 inches] is adequate to demonstrate motion without exceeding the alignment limit when only one CEA is being moved. The 92 day Frequency takes into consideration other information available to the operator in the control room and other surveillances being performed more frequently, which add to the determination of OPERABILITY of the CEAs. Between required performances of SR 3.1.4.4, if a CEA(s) is discovered to be immovable, but remains trippable, the CEA is considered to be OPERABLE. At any time, if a CEA(s) is immovable, a determination of the trippability (OPERABILITY) of the CEA(s) must be made, and appropriate action taken.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.1.4.5

Performance of a CHANNEL FUNCTIONAL TEST of each reed switch position transmitter channel ensures the channel is OPERABLE and capable of indicating CEA position over the entire length of the CEA's travel. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions. Since this Surveillance must be performed when the reactor is shut down, an 18 month Frequency to be coincident with refueling outage was selected. Operating experience has shown that these components usually pass this Surveillance when performed at a Frequency of once every 18 months. Furthermore, the Frequency takes into account other surveillances being performed at shorter Frequencies, which determine the OPERABILITY of the CEA Reed Switch Indication System.

SR 3.1.4.6

Verification of CEA drop times determined that the maximum CEA drop time permitted is consistent with the assumed drop time used in that safety analysis (Ref. 7). Measuring drop times prior to reactor criticality, after reactor vessel head removal, ensures that reactor internals and CEDM will not interfere with CEA motion or drop time and that no degradation in these systems has occurred that would adversely affect CEA motion or drop time. Individual CEAs whose drop times are greater than safety analysis assumptions are not OPERABLE. This SR is performed prior to criticality, based on the need to perform this Surveillance under the conditions that apply during a unit outage and because of the potential for an unplanned unit transient if the Surveillance were performed with the reactor at power.

BASES

REFERENCES	1.	10 CFR 50, Appendix A, GDC 10 and GDC 26.
	2.	10 CFR 50.46.
	3.	FSAR, Section [ ].
	4.	FSAR, Section [ ].
	5.	FSAR, Section [ ].
	6.	FSAR, Section [ ].
	7.	FSAR, Section [ ].

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.5 Shutdown Control Element Assembly (CEA) Insertion Limits (Analog)

BASES

BACKGROUND

The insertion limits of the shutdown Control Element Assemblies (CEAs) are initial assumptions in all safety analyses that assume CEA insertion upon reactor trip. The insertion limits directly affect core power distributions and assumptions of available SDM, ejected CEA worth, and initial reactivity insertion rate.

The applicable criteria for these reactivity and power distribution design requirements are 10 CFR 50, Appendix A, GDC 10, "Reactor Design," and GDC 26, "Reactivity Limits" (Ref. 1), and 10 CFR 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Nuclear Power Reactors" (Ref. 2). Limits on shutdown CEA insertion have been established, and all CEA positions are monitored and controlled during power operation to ensure that the reactivity limits, ejected CEA worth, and SDM limits are preserved.

The shutdown CEAs are arranged into groups that are radially symmetric. Therefore, movement of the shutdown CEAs does not introduce radial asymmetries in the core power distribution. The shutdown and regulating CEAs provide the required reactivity worth for immediate reactor shutdown upon a reactor trip.

The design calculations are performed with the assumption that the shutdown CEAs are withdrawn prior to the regulating CEAs. The shutdown CEAs can be fully withdrawn without the core going critical. This provides available negative reactivity for SDM in the event of boration errors. The shutdown CEAs are controlled manually or automatically by the control room operator. During normal unit operation, the shutdown CEAs are fully withdrawn. The shutdown CEAs must be completely withdrawn from the core prior to withdrawing any regulating CEAs during an approach to criticality. The shutdown CEAs are then left in this position until the reactor is shut down. They affect core power, burnup distribution, and add negative reactivity to shut down the reactor upon receipt of a reactor trip signal.

APPLICABLE SAFETY ANALYSES

Accident analysis assumes that the shutdown CEAs are fully withdrawn any time the reactor is critical. This ensures that:

a. The minimum SDM is maintained and

b. The potential effects of a CEA ejection accident are limited to acceptable limits.

BASES

APPLICABLE SAFETY ANALYSES (continued)

CEAs are considered fully withdrawn at 129 inches, since this position places them outside the active region of the core.

On a reactor trip, all CEAs (shutdown and regulating), except the most reactive CEA, are assumed to insert into the core. The shutdown and regulating CEAs shall be at their insertion limits and available to insert the maximum amount of negative reactivity on a reactor trip signal. The regulating CEAs may be partially inserted in the core as allowed by LCO 3.1.6, "Regulating Control Element Assembly (CEA) Insertion Limits." The shutdown CEA insertion limit is established to ensure that a sufficient amount of negative reactivity is available to shut down the reactor and maintain the required SDM (see LCO 3.1.1, "SHUTDOWN MARGIN (SDM)") following a reactor trip from full power. The combination of regulating CEAs and shutdown CEAs (less the most reactive CEA, which is assumed to be fully withdrawn) is sufficient to take the reactor from full power conditions at rated temperature to zero power, and to maintain the required SDM at rated no load temperature (Ref. 3). The shutdown CEA insertion limit also limits the reactivity worth of an ejected shutdown CEA.

The acceptance criteria for addressing shutdown CEA as well as regulating CEA insertion limits and inoperability or misalignment are that:

a. There be no violation of either:

   1. Specified acceptable fuel design limits or

   2. Reactor Coolant System pressure boundary damage and

b. The core remains subcritical after accident transients.

As such, the shutdown CEA insertion limits affect safety analyses involving core reactivity, ejected CEA worth, and SDM (Ref. 3).

The shutdown CEA insertion limits satisfy Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

The shutdown CEAs must be within their insertion limits any time the reactor is critical or approaching criticality. This ensures that a sufficient amount of negative reactivity is available to shut down the reactor and maintain the required SDM following a reactor trip.

BASES

APPLICABILITY

The shutdown CEAs must be within their insertion limits, with the reactor in MODES 1 and 2. The Applicability in MODE 2 begins anytime any regulating CEA is not fully inserted. This ensures that a sufficient amount of negative reactivity is available to shut down the reactor and maintain the required SDM following a reactor trip. In MODE 3, 4, 5, or 6, the shutdown CEAs are fully inserted in the core and contribute to the SDM. Refer to LCO 3.1.1, "SHUTDOWN MARGIN (SDM)," for SDM requirements in MODES 3, 4, and 5. LCO 3.9.1, "Boron Concentration," ensures adequate SDM in MODE 6.

This LCO has been modified by a Note indicating the LCO requirement is suspended during SR 3.1.4.4. This SR verifies the freedom of the CEAs to move, and requires the shutdown CEAs to move below the LCO limits, which would normally violate the LCO.

ACTIONS

A.1

Prior to entering this condition, the shutdown CEAs were fully withdrawn. If a shutdown CEA(s) is then inserted into the core, its potential negative reactivity is added to the core as it is inserted.

If the CEA(s) is not restored to within limits within 1 hour, then an additional 1 hour is allowed for restoring the CEA(s) to within limits. The 2 hour total Completion Time allows the operator adequate time to adjust the CEA(s) in an orderly manner and is consistent with the required Completion Times in LCO 3.1.4, "Control Element Assembly (CEA) Alignment."

B.1

When Required Action A.1 or A.2 cannot be met or completed within the required Completion Time, a controlled shutdown should be commenced. The allowed Completion Time of 6 hours is reasonable, based on operating experience, for reaching MODE 3 from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.1.5.1

Verification that the shutdown CEAs are within their insertion limits prior to an approach to criticality ensures that when the reactor is critical, or being taken critical, the shutdown CEAs will be available to shut down the reactor, and the required SDM will be maintained following a reactor trip. This SR and Frequency ensure that the shutdown CEAs are withdrawn before the regulating CEAs are withdrawn during a unit startup.

BASES

SURVEILLANCE REQUIREMENTS (continued)

Since the shutdown CEAs are positioned manually by the control room operator, verification of shutdown CEA position at a Frequency of 12 hours is adequate to ensure that the shutdown CEAs are within their insertion limits. Also, the 12 hour Frequency takes into account other information available to the operator in the control room for the purpose of monitoring the status of the shutdown CEAs.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 10 and GDC 26.
2. 10 CFR 50.46.
3. FSAR, Section [ ].

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.6 Regulating Control Element Assembly (CEA) Insertion Limits (Analog)

BASES

BACKGROUND

The insertion limits of the regulating Control Element Assemblies (CEAs) are initial assumptions in all safety analyses that assume CEA insertion upon reactor trip. The insertion limits directly affect core power distributions, assumptions of available SDM, and initial reactivity insertion rate. The applicable criteria for these reactivity and power distribution design requirements are 10 CFR 50, Appendix A, GDC 10, "Reactor Design," and GDC 26, "Reactivity Limits" (Ref. 1), and 10 CFR 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Nuclear Power Reactors" (Ref. 2).

Limits on regulating CEA insertion have been established, and all CEA positions are monitored and controlled during power operation to ensure that the power distribution and reactivity limits defined by the design power peaking, ejected CEA worth, reactivity insertion rate, and SDM limits are preserved.

The regulating CEA groups operate with a predetermined amount of position overlap, in order to approximate a linear relation between CEA worth and CEA position (integral CEA worth). The regulating CEA groups are withdrawn and operate in a predetermined sequence. The group sequence and overlap limits are specified in the COLR.

The regulating CEAs are used for precise reactivity control of the reactor. The positions of the regulating CEAs are manually controlled. They are capable of adding reactivity very quickly (compared to borating or diluting).

The power density at any point in the core must be limited to maintain specified acceptable fuel design limits, including limits that preserve the criteria specified in 10 CFR 50.46 (Ref. 2). Together, LCO 3.1.6, LCO 3.2.4, "AZIMUTHAL POWER TILT (Tq)," and LCO 3.2.5, "AXIAL SHAPE INDEX (ASI)," provide limits on control component operation and on monitored process variables to ensure the core operates within the linear heat rate (LCO 3.2.1, "Linear Heat Rate (LHR)"), total planar radial peaking factor (F^T_{XY}) (LCO 3.2.2, "Total Planar Radial Peaking Factor (F^T_{XY})"), and total integrated radial peaking factor (F^T_r) (LCO 3.2.3, "Total Integrated Radial Peaking Factor (F^T_r)") limits in the COLR. Operation within the LHR limits given in the COLR prevents power peaks that would exceed the loss of coolant accident (LOCA) limits derived by the Emergency Core Cooling System analysis. Operation within the F^T_{XY} and

BASES

BACKGROUND (continued)

F_r^T limits given in the COLR prevents departure from nucleate boiling (DNB) during a loss of forced reactor coolant flow accident. In addition to the LHR, F_{XY}^T, and $F^T{}_r$ limits, certain reactivity limits are preserved by regulating CEA insertion limits. The regulating CEA insertion limits also restrict the ejected CEA worth to the values assumed in the safety analysis and preserve the minimum required SDM in MODES 1 and 2.

The establishment of limiting safety system settings and LCOs requires that the expected long and short term behavior of the radial peaking factors be determined. The long term behavior relates to the variation of the steady state radial peaking factors with core burnup and is affected by the amount of CEA insertion assumed, the portion of a burnup cycle over which such insertion is assumed, and the expected power level variation throughout the cycle. The short term behavior relates to transient perturbations to the steady state radial peaks, due to radial xenon redistribution. The magnitudes of such perturbations depend upon the expected use of the CEAs during anticipated power reductions and load maneuvering. Analyses are performed, based on the expected mode of operation of the Nuclear Steam Supply System (base loaded, maneuvering, etc.). From these analyses, CEA insertions are determined and a consistent set of radial peaking factors defined. The long term steady state and short term insertion limits are determined, based upon the assumed mode of operation used in the analyses, and provide a means of preserving the assumption on CEA insertions used. The long and short term insertion limits of LCO 3.1.6 are specified for the plant, which has been designed primarily for base loaded operation, but has the ability to accommodate a limited amount of load maneuvering.

The regulating CEA insertion and alignment limits are process variables that together characterize and control the three dimensional power distribution of the reactor core. Additionally, the regulating bank insertion limits control the reactivity that could be added in the event of a CEA ejection accident, and the shutdown and regulating bank insertion limits ensure the required SDM is maintained.

Operation within the subject LCO limits will prevent fuel cladding failures that would breach the primary fission product barrier and release fission products to the reactor coolant in the event of a LOCA, loss of flow, ejected CEA, or other accident requiring termination by a Reactor Protection System trip function.

BASES

APPLICABLE SAFETY ANALYSES

The fuel cladding must not sustain damage as a result of normal operation (Condition I) and anticipated operational occurrences (Condition II). The acceptance criteria for the regulating CEA insertion, ASI, and T_q LCOs are such as to preclude core power distributions from occurring that would violate the following fuel design criteria:

a. During a large break LOCA, the peak cladding temperature must not exceed a limit of 2200°F, 10 CFR 50.46 (Ref. 2),

b. During a loss of forced reactor coolant flow accident, there must be at least a 95% probability at a 95% confidence level (the 95/95 DNB criterion) that the hot fuel CEA in the core does not experience a DNB condition,

c. During an ejected CEA accident, the fission energy input to the fuel must not exceed 280 cal/gm (Ref. 3), and

d. The CEAs must be capable of shutting down the reactor with a minimum required SDM, with the highest worth CEA stuck fully withdrawn, GDC 26 (Ref. 1).

Regulating CEA position, ASI, and T_q are process variables that together characterize and control the three dimensional power distribution of the reactor core.

Fuel cladding damage does not occur when the core is operated outside these LCOs during normal operation. However, fuel cladding damage could result, should an accident occur with simultaneous violation of one or more of these LCOs. Changes in the power distribution can cause increased power peaking and corresponding increased local LHRs.

The SDM requirement is ensured by limiting the regulating and shutdown CEA insertion limits, so that the allowable inserted worth of the CEAs is such that sufficient reactivity is available to shut down the reactor to hot zero power. SDM assumes the maximum worth CEA remains fully withdrawn upon trip (Ref. 4).

The most limiting SDM requirements for MODE 1 and 2 conditions at BOC are determined by the requirements of several transients, e.g., loss of flow, seized rotor, etc. However, the most limiting SDM requirements for MODES 1 and 2 at EOC come from just one transient, Steam Line Break (SLB). The requirements of the SLB event at EOC for both the full power and no load conditions are significantly larger than those of any other event at that time in cycle and, also, considerably larger than the most limiting requirements at BOC.

BASES

APPLICABLE SAFETY ANALYSES (continued)

Although the most limiting SDM requirements at EOC are much larger than those at BOC, the available SDMs obtained via the scramming of the CEAs are also substantially larger due to the much lower boron concentration at EOC. To verify that adequate SDMs are available throughout the cycle to satisfy the changing requirements, calculations are performed at both BOC and EOC. It has been determined that calculations at these two times in cycle are sufficient since the differences between available SDMs and the limiting SDM requirements are the smallest at these times in cycle. The measurement of CEA bank worth performed as part of the Startup Testing Program demonstrates that the core has the expected shutdown capability. Consequently, adherance to LCOs 3.1.5 and 3.1.6 provides assurance that the available SDMs at any time in cycle will exceed the limiting SDM requirements at that time in cycle.

Operation at the insertion limits or ASI limits may approach the maximum allowable linear heat generation rate or peaking factor, with the allowed T_q present. Operation at the insertion limit may also indicate the maximum ejected CEA worth could be equal to the limiting value in fuel cycles that have sufficiently high ejected CEA worths.

The regulating and shutdown CEA insertion limits ensure that safety analyses assumptions for reactivity insertion rate, SDM, ejected CEA worth, and power distribution peaking factors are preserved (Ref. 5).

The regulating CEA insertion limits satisfy Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

The limits on regulating CEAs sequence, overlap, and physical insertion, as defined in the COLR, must be maintained because they serve the function of preserving power distribution, ensuring that the SDM is maintained, ensuring that ejected CEA worth is maintained, and ensuring adequate negative reactivity insertion on trip. The overlap between regulating banks provides more uniform rates of reactivity insertion and withdrawal and is imposed to maintain acceptable power peaking during regulating CEA motion.

The power dependent insertion limit (PDIL) alarm circuit is required to be OPERABLE for notification that the CEAs are outside the required insertion limits. When the PDIL alarm circuit is inoperable, the verification of CEA positions is increased to ensure improper CEA alignment is identified before unacceptable flux distribution occurs.

BASES

APPLICABILITY

The regulating CEA sequence, overlap, and physical insertion limits shall be maintained with the reactor in MODES 1 and 2. These limits must be maintained, since they preserve the assumed power distribution, ejected CEA worth, SDM, and reactivity rate insertion assumptions. Applicability in MODES 3, 4, and 5 is not required, since neither the power distribution nor ejected CEA worth assumptions would be exceeded in these MODES. SDM is preserved in MODES 3, 4, and 5 by adjustments to the soluble boron concentration.

This LCO has been modified by a Note indicating the LCO requirement is suspended during SR 3.1.4.4. This SR verifies the freedom of the CEAs to move, and requires the regulating CEAs to move below the LCO limits, which would normally violate the LCO. The Note also allows the LCO to be not applicable during reactor power cutback operation, which inserts a selected CEA group (usually group 5) during loss of load events.

ACTIONS

A.1 and A.2

Operation beyond the transient insertion limit may result in a loss of SDM and excessive peaking factors. The transient insertion limit should not be violated during normal operation; this violation, however, may occur during transients when the operator is manually controlling the CEAs in response to changing plant conditions. When the regulating groups are inserted beyond the transient insertion limits, actions must be taken to either withdraw the regulating groups beyond the limits or to reduce THERMAL POWER to less than or equal to that allowed for the actual CEA insertion limit. Two hours provides a reasonable time to accomplish this, allowing the operator to deal with current plant conditions while limiting peaking factors to acceptable levels.

B.1 and B.2

If the CEAs are inserted between the long term steady state insertion limits and the transient insertion limits for intervals > 4 hours per 24 hour period, and the short term steady state insertions are exceeded, peaking factors can develop that are of immediate concern (Ref. 6).

Verifying the short term steady state insertion limits are not exceeded ensures that the peaking factors that do develop are within those allowed for continued operation. Fifteen minutes provides adequate time for the operator to verify if the short term steady state insertion limits are exceeded.

BASES

ACTIONS (continued)

Experience has shown that rapid power increases in areas of the core, in which the flux has been depressed, can result in fuel damage, as the LHR in those areas rapidly increases. Restricting the rate of THERMAL POWER increases to ≤ 5% RTP per hour, following CEA insertion beyond the long term steady state insertion limits, ensures the power transients experienced by the fuel will not result in fuel failure (Ref. 7).

C.1

With the regulating CEAs inserted between the long term steady state insertion limit and the transient insertion limit, and with the core approaching the 5 effective full power days (EFPD) per 30 EFPD or 14 EFPD per 365 EFPD limits, the core approaches the acceptable limits placed on operation with flux patterns outside those assumed in the long term burnup assumptions (Ref. 8). In this case, the CEAs must be returned to within the long term steady state insertion limits, or the core must be placed in a condition in which the abnormal fuel burnup cannot continue. A Completion Time of 2 hours is allotted to return the CEAs to within the long term steady state insertion limits.

The required Completion Time of 2 hours from initial discovery of a regulating CEA group outside the limits until its restoration to within the long term steady state limits, shown on the figures in the COLR, allows sufficient time for borated water to enter the Reactor Coolant System from the chemical addition and makeup systems, and to cause the regulating CEAs to withdraw to the acceptable region. It is reasonable to continue operation for 2 hours after it is discovered that the 5 day or 14 day EFPD limit has been exceeded. This Completion Time is based on limiting the potential xenon redistribution, the low probability of an accident, and the steps required to complete the action.

D.1

When the PDIL alarm circuit is inoperable, performing SR 3.1.6.1 within 1 hour and once per 4 hours thereafter ensures improper CEA alignments are identified before unacceptable flux distributions occur.

BASES

ACTIONS (continued)

E.1

When a Required Action cannot be completed within the required Completion Time, a controlled shutdown should be commenced. The allowed Completion Time of 6 hours is reasonable, based on operating experience, for reaching MODE 3 from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.1.6.1

With the PDIL alarm circuit OPERABLE, verification of each regulating CEA group position every 12 hours is sufficient to detect CEA positions that may approach the acceptable limits, and to provide the operator with time to undertake the Required Action(s) should the sequence or insertion limits be found to be exceeded. The 12 hour Frequency also takes into account the indication provided by the PDIL alarm circuit and other information about CEA group positions available to the operator in the control room.

SR 3.1.6.1 is modified by a Note indicating that entry is allowed into MODE 2 for 12 hours without having performed the SR. This is necessary, since the unit must be in the applicable MODES in order to perform Surveillances that demonstrate the LCO limits are met.

SR 3.1.6.2

Verification of the accumulated time of CEA group insertion between the long term steady state insertion limits and the transient insertion limits ensures the cumulative time limits are not exceeded. The 24 hour Frequency ensures the operator identifies a time limit that is being approached before it is reached.

SR 3.1.6.3

Demonstrating the PDIL alarm circuit OPERABLE verifies that the PDIL alarm circuit is functional. The 31 day Frequency takes into account other Surveillances being performed at shorter Frequencies that identify improper CEA alignments.

BASES

REFERENCES

1. 10 CFR 50, Appendix A, GDC 10 and GDC 26.
2. 10 CFR 50.46
3. FSAR, Section [ ], Section [ ], and Section [ ].
4. FSAR, Section [ ].
5. FSAR, Section [ ].
6. FSAR, Section [ ].
7. FSAR, Section [ ].
8. FSAR, Section [ ].

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.7 Special Test Exception (STE) - SHUTDOWN MARGIN (SDM) (Analog)

BASES

BACKGROUND

The primary purpose of the SHUTDOWN MARGIN (SDM) Special Test Exception (STE) is to permit relaxation of existing LCOs to allow the performance of certain PHYSICS TESTS. These tests are constructed to determine the control element assembly (CEA) worth.

Section XI of 10 CFR 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Processing Plants" (Ref. 1), requires that a test program be established to ensure that structures, systems, and components will perform satisfactorily in service. All functions necessary to ensure that specified design conditions are not exceeded during normal operation and anticipated operational occurrences must be tested. Testing is required as an integral part of the design, fabrication, construction, and operation of the power plant. Requirements for notification of the NRC, for the purpose of conducting tests and experiments, are specified in 10 CFR 50.59, "Changes, Tests, and Experiments" (Ref. 2).

The key objectives of a test program are to (Ref. 3):

a. Ensure that the facility has been adequately designed,

b. Validate the analytical models used in design and analysis,

c. Verify assumptions used for predicting plant response,

d. Ensure that installation of equipment in the facility has been accomplished in accordance with the design, and

e. Verify that operating and emergency procedures are adequate.

To accomplish these objectives, testing is required prior to initial criticality, after each refueling shutdown, and during startup, low power operation, power ascension, and at power operation. The PHYSICS TESTS requirements for reload fuel cycles ensure that the operating characteristics of the core are consistent with the design predictions, and that the core can be operated as designed (Ref. 4).

BASES

BACKGROUND (continued)

PHYSICS TESTS procedures are written and approved in accordance with established formats. The procedures include all information necessary to permit a detailed execution of testing required to ensure that the design intent is met. PHYSICS TESTS are performed in accordance with these procedures, and test results are approved prior to continued power escalation and long term power operation. Examples of PHYSICS TESTS include determination of critical boron concentration, CEA group worths, reactivity coefficients, flux symmetry, and core power distribution.

APPLICABLE SAFETY ANALYSES

It is acceptable to suspend certain LCOs for PHYSICS TESTS because fuel damage criteria are not exceeded. Even if an accident occurs during PHYSICS TESTS with one or more LCOs suspended, fuel damage criteria are preserved because adequate limits on power distribution and shutdown capability are maintained during PHYSICS TESTS.

Reference 5 defines the requirements for initial testing of the facility, including PHYSICS TESTS. Requirements for reload fuel cycle PHYSICS TESTS are defined in ANSI/ANS-19.6.1-1985 (Ref. 4). Although these PHYSICS TESTS are generally accomplished within the limits of all LCOs, conditions may occur when one or more LCOs must be suspended to make completion of PHYSICS TESTS possible or practical. This is acceptable as long as the fuel design criteria are not violated. As long as the linear heat rate (LHR) remains within its limit, fuel design criteria are preserved.

In this test, the following LCOs are suspended:

a. LCO 3.1.1, "SHUTDOWN MARGIN (SDM)",

b. LCO 3.1.5, “Shutdown Control Element Assembly (CEA) Insertion Limits,” and

c. LCO 3.1.6, "Regulating Control Element Assembly (CEA) Insertion Limits."

Therefore, this LCO places limits on the minimum amount of CEA worth required to be available for reactivity control when CEA worth measurements are performed.

The individual LCOs cited above govern SDM CEA group height, insertion, and alignment. Additionally, the LCOs governing Reactor Coolant System (RCS) flow, reactor inlet temperature, and pressurizer pressure contribute to maintaining departure from nucleate boiling (DNB) parameter limits. The initial condition criteria for accidents sensitive to

BASES

APPLICABLE SAFETY ANALYSES (continued)

core power distribution are preserved by the LHR and DNB parameter limits. The criteria for the loss of coolant accident (LOCA) are specified in 10 CFR 50.46, "Acceptance Criteria for Emergency core Cooling Systems for Light Water Nuclear Power Reactors" (Ref. 6). The criteria for the loss of forced reactor coolant flow accident are specified in Reference 7. Operation within the LHR limit preserves the LOCA criteria; operation within the DNB parameter limits preserves the loss of flow criteria.

SRs are conducted as necessary to ensure that LHR and DNB parameters remain within limits during PHYSICS TESTS. Performance of these SRs allows PHYSICS TESTS to be conducted without decreasing the margin of safety.

Requiring that shutdown reactivity equivalent to at least the highest estimated CEA worth (of those CEAs actually withdrawn) be available for trip insertion from the OPERABLE CEA provides a high degree of assurance that shutdown capability is maintained for the most challenging postulated accident, a stuck CEA. Since LCO 3.1.1 is suspended, however, there is not the same degree of assurance during this test that the reactor would always be shut down if the highest worth CEA was stuck out and calculational uncertainties or the estimated highest CEA worth was not as expected (the single failure criterion is not met). This situation is judged acceptable, however, because specified acceptable fuel damage limits are still met. The risk of experiencing a stuck CEA and subsequent criticality is reduced during this PHYSICS TEST exception by the requirements to determine CEA positions every 2 hours; by the trip of each CEA to be withdrawn 24 hours prior to suspending the SDM; and by ensuring that shutdown reactivity is available, equivalent to the reactivity worth of the estimated highest worth withdrawn CEA (Ref. 5).

PHYSICS TESTS include measurement of core parameters or exercise of control components that affect process variables. Among the process variables involved are total planar radial peaking factor, total integrated radial peaking factor, T_q and ASI, which represent initial condition input (power peaking) to the accident analysis. Also involved are the shutdown and regulating CEAs, which affect power peaking and are required for shutdown of the reactor. The limits for these variables are specified for each fuel cycle in the COLR.

As described in LCO 3.0.7, compliance with Special Test Exception LCOs is optional, and therefore no criteria of 10 CFR 50.36(c)(2)(ii) apply. Special Test Exception LCOs provide flexibility to perform certain operations by appropriately modifying requirements of other LCOs. A discussion of the criteria satisfied for the other LCOs is provided in their respective Bases.

BASES

LCO	This LCO provides that a minimum amount of CEA worth is immediately available for reactivity control when CEA worth measurement tests are performed. The STE is required to permit the periodic verification of the actual versus predicted worth of the regulating and shutdown CEAs. The SDM requirements of LCO 3.1.1, the shutdown CEA insertion limits of LCO 3.1.5, and the regulating CEA insertion limits of LCO 3.1.6 may be suspended.
APPLICABILITY	This LCO is applicable in MODES 2 and 3. Although CEA worth testing is conducted in MODE 2, sufficient negative reactivity is inserted during the performance of these tests to result in temporary entry into MODE 3. Because the intent is to immediately return to MODE 2 to continue CEA worth measurements, the STE allows limited operation to 6 consecutive hours in MODE 3, as indicated by the Note, without having to borate to meet the SDM requirements of LCO 3.1.1.
ACTIONS	<u>A.1</u> With any CEA not fully inserted and less than the minimum required reactivity equivalent available for insertion, or with all CEAs inserted and the reactor subcritical by less than the reactivity equivalent of the highest worth CEA, restoration of the minimum SDM requirements must be accomplished by increasing the RCS boron concentration. The required Completion Time of 15 minutes for initiating boration allows the operator sufficient time to align the valves and start the boric acid pumps and is consistent with the Completion Time of LCO 3.1.1.
SURVEILLANCE REQUIREMENTS	<u>SR 3.1.7.1</u> Verification of the position of each partially or fully withdrawn full length or part length CEA is necessary to ensure that the minimum negative reactivity requirements for insertion on a trip are preserved. A 2 hour Frequency is sufficient for the operator to verify that each CEA position is within the acceptance criteria. <u>SR 3.1.7.2</u> Prior demonstration that each CEA to be withdrawn from the core during PHYSICS TESTS is capable of full insertion, when tripped from at least a 50% withdrawn position, ensures that the CEA will insert on a trip signal. The Frequency ensures that the CEAs are OPERABLE prior to reducing SDM to less than the limits of LCO 3.1.1.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The SR is modified by a Note which allows the SR to not be performed during initial power escalation following a refueling outage if SR 3.1.4.6 has been met during that refueling outage. This allows the CEA drop time test, which also proves the CEAs are trippable, to be credited for this SR.

REFERENCES

1. 10 CFR 50, Appendix B, Section XI.
2. 10 CFR 50.59.
3. Regulatory Guide 1.68, Revision 2, August 1978.
4. ANSI/ANS-19.6.1-1985, December 13, 1985.
5. FSAR, Chapter [14].
6. 10 CFR 50.46.
7. FSAR, Chapter [15].

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.8 Special Test Exceptions (STE) - MODES 1 and 2 (Analog)

BASES

BACKGROUND

The primary purpose of these MODES 1 and 2 Special Test Exceptions (STE) is to permit relaxation of existing LCOs to allow the performance of certain PHYSICS TESTS. These tests are conducted to determine specific reactor core characteristics.

Section XI of 10 CFR 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Processing Plants" (Ref. 1), requires that a test program be established to ensure that structures, systems, and components will perform satisfactorily in service. All functions necessary to ensure that specified design conditions are not exceeded during normal operation and anticipated operational occurrences must be tested. Testing is required as an integral part of the design, fabrication, construction, and operation of the power plant. Requirements for notification of the NRC, for the purpose of conducting tests and experiments, are specified in 10 CFR 50.59, "Changes, Tests, and Experiments" (Ref. 2).

The key objectives of a test program are to (Ref. 3):

a. Ensure that the facility has been adequately designed,

b. Validate the analytical models used in design and analysis,

c. Verify assumptions used for predicting plant response,

d. Ensure that installation of equipment in the facility has been accomplished in accordance with design, and

e. Verify that operating and emergency procedures are adequate.

To accomplish these objectives, testing is required prior to initial criticality, after each refueling shutdown, and during startup, low power operation, power ascension, and at power operation. The PHYSICS TESTS requirements for reload fuel cycles ensure that the operating characteristics of the core are consistent with the design predictions, and that the core can be operated as designed (Ref. 4).

BASES

BACKGROUND (continued)

PHYSICS TESTS procedures are written and approved in accordance with established formats. The procedures include all information necessary to permit a detailed execution of testing required to ensure that design intent is met. PHYSICS TESTS are performed in accordance with these procedures and test results are approved prior to continued power escalation and long term power operation.

Examples of PHYSICS TESTS include determination of critical boron concentration, control element assembly (CEA) group worths, reactivity coefficients, flux symmetry, and core power distribution.

APPLICABLE SAFETY ANALYSES

It is acceptable to suspend certain LCOs for PHYSICS TESTS because fuel damage criteria are not exceeded. Even if an accident occurs during a PHYSICS TEST with one or more LCOs suspended, fuel damage criteria are preserved because the limits on power distribution and shutdown capability are maintained during PHYSICS TESTS.

Reference 5 defines the requirements for initial testing of the facility, including PHYSICS TESTS. Requirements for reload fuel cycle PHYSICS TESTS are defined in ANSI/ANS-19.6.1-1985 (Ref. 4). Although these PHYSICS TESTS are generally accomplished within the limits of all LCOs, conditions may occur when one or more LCOs must be suspended to make completion of PHYSICS TESTS possible or practical. This is acceptable as long as the fuel design criteria are not violated. As long as the linear heat rate (LHR) remains within its limit, fuel design criteria are preserved.

In this test, the following LCOs are suspended:

LCO 3.1.3, "Moderator Temperature Coefficient (MTC),"
LCO 3.1.4, "Control Element Assembly (CEA) Alignment,"
LCO 3.1.5, "Shutdown Control Element Assembly (CEA) Insertion Limits,"
LCO 3.1.6, "Regulating Control Element Assembly (CEA) Insertion Limits,"
LCO 3.2.2, "Total Planar Radial Peaking Factor (F^T_{XY}),"
LCO 3.2.3, "Total Integrated Radial Peaking Factor (F^T_r)" and
LCO 3.2.4, "AZIMUTHAL POWER TILT (T_q)."

The safety analysis (Ref. 6) places limits on allowable THERMAL POWER during PHYSICS TESTS and requires the LHR and the departure from nucleate boiling (DNB) parameter to be maintained within limits. The power plateau of < 85% RTP and the associated trip setpoints are required to ensure [explain].

BASES

APPLICABLE SAFETY ANALYSES (continued)

The individual LCOs governing CEA group height, insertion and alignment, ASI, F^T_{XY}, F^T_r, and T_q preserve the LHR limits. Additionally, the LCOs governing Reactor Coolant System (RCS) flow, reactor inlet temperature (T_c), and pressurizer pressure contribute to maintaining DNB parameter limits. The initial condition criteria for accidents sensitive to core power distribution are preserved by the LHR and DNB parameter limits. The criteria for the loss of coolant accident (LOCA) are specified in 10 CFR 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Nuclear Power Reactors" (Ref. 7). The criteria for the loss of forced reactor coolant flow accident are specified in Reference 7. Operation within the LHR limit preserves the LOCA criteria; operation within the DNB parameter limits preserves the loss of flow criteria.

During PHYSICS TESTS, one or more of the LCOs that normally preserve the LHR and DNB parameter limits may be suspended. The results of the accident analysis are not adversely impacted, however, if LHR and DNB parameters are verified to be within their limits while the LCOs are suspended. Therefore, SRs are placed as necessary to ensure that LHR and DNB parameters remain within limits during PHYSICS TESTS. Performance of these Surveillances allows PHYSICS TESTS to be conducted without decreasing the margin of safety.

PHYSICS TESTS include measurement of core parameters or exercise of control components that affect process variables. Among the process variables involved are F^T_{XY}, F^T_r, T_q, and ASI, which represent initial condition input (power peaking) to the accident analysis. Also involved are the shutdown and regulating CEAs, which affect power peaking and are required for shutdown of the reactor. The limits for these variables are specified for each fuel cycle in the COLR.

As described in LCO 3.0.7, compliance with Special Test Exceptions LCOs is optional, and therefore no criteria of 10 CFR 50.36(c)(2)(ii) apply. Special Test Exception LCOs provide flexibility to perform certain operations by appropriately modifying requirements of other LCOs. A discussion of the criteria satisfied for the other LCOs is provided in their respective Bases.

BASES

LCO

This LCO permits individual CEAs to be positioned outside of their normal group heights and insertion limits during the performance of PHYSICS TESTS such as those required to:

a. Measure CEA worth,

b. Determine the reactor stability index and damping factor under xenon oscillation conditions,

c. Determine power distributions for nonnormal CEA configurations,

d. Measure rod shadowing factors, and

e. Measure temperature and power coefficients.

Additionally, it permits the center CEA to be misaligned during PHYSICS TESTS required to determine the isothermal temperature coefficient (ITC), MTC, and power coefficient.

The requirements of LCO 3.1.3, LCO 3.1.4, LCO 3.1.5, LCO 3.1.6, LCO 3.2.2, LCO 3.2.3, and LCO 3.2.4 may be suspended during the performance of PHYSICS TESTS, provided THERMAL POWER is restricted to test power plateau, which shall not exceed 85% RTP.

APPLICABILITY

This LCO is applicable in MODES 1 and 2 because the reactor must be critical at various THERMAL POWER levels to perform the PHYSICS TESTS described in the LCO section. Limiting the test power plateau to < 85% RTP ensures that LHRs are maintained within acceptable limits.

ACTIONS

A.1

If THERMAL POWER exceeds the test power plateau, THERMAL POWER must be reduced to restore the additional thermal margin provided by the reduction. The 15 minute Completion Time ensures that prompt action shall be taken to reduce THERMAL POWER to within acceptable limits.

B.1 and B.2

If Required Action A.1 cannot be completed within the required Completion Time, PHYSICS TESTS must be suspended within 1 hour. Allowing 1 hour for suspending PHYSICS TESTS allows the operator sufficient time to change any abnormal CEA configuration back to within the limits of LCO 3.1.4, LCO 3.1.5, and LCO 3.1.6.

BASES

ACTIONS (continued)

Suspension of PHYSICS TESTS exceptions requires restoration of each of the applicable LCOs to within specification.

SURVEILLANCE REQUIREMENTS

SR 3.1.8.1

Verifying that THERMAL POWER is equal to or less than that allowed by the test power plateau, as specified in the PHYSICS TEST procedure and required by the safety analysis, ensures that adequate LHR and DNB parameter margins are maintained while LCOs are suspended. The 1 hour Frequency is sufficient, based on the slow rate of power change and increased operational controls in place during PHYSICS TESTS.

REFERENCES

1. 10 CFR 50, Appendix B, Section XI.
2. 10 CFR 50.59.
3. Regulatory Guide 1.68, Revision 2, August 1978.
4. ANSI/ANS-19.6.1-1985, December 13, 1985.
5. FSAR, Chapter [14].
6. FSAR, Section [15.3.2.1].
7. 10 CFR 50.46.

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.1 SHUTDOWN MARGIN (SDM) (Digital)

BASES

BACKGROUND

The reactivity control systems must be redundant and capable of holding the reactor core subcritical when shutdown under cold conditions, in accordance with GDC 26 (Ref. 1). Maintenance of the SHUTDOWN MARGIN (SDM) ensures that postulated reactivity events will not damage the fuel. SDM requirements provide sufficient reactivity margin to ensure that acceptable fuel design limits will not be exceeded for normal shutdown and anticipated operational occurrences (AOOs). As such, the SDM defines the degree of subcriticality that would be obtained immediately following the insertion of all full length control element assemblies (CEAs), assuming the single CEA of highest reactivity worth is fully withdrawn.

The system design requires that two independent reactivity control systems be provided, and that one of these systems be capable of maintaining the core subcritical under cold conditions. These requirements are provided by the use of movable CEAs and soluble boric acid in the Reactor Coolant System (RCS). The CEA System provides the SDM during power operation and is capable of making the core subcritical rapidly enough to prevent exceeding acceptable fuel damage limits, assuming that the CEA of highest reactivity worth remains fully withdrawn.

The soluble boron system can compensate for fuel depletion during operation and all xenon burnout reactivity changes, and maintain the reactor subcritical under cold conditions.

During power operation, SDM control is ensured by operating with the shutdown CEAs fully withdrawn and the regulating CEAs within the limits of LCO 3.1.6, "Regulating Control Element Assembly (CEA) Insertion Limits." When the unit is in the shutdown and refueling modes, the SDM requirements are met by means of adjustments to the RCS boron concentration.

APPLICABLE SAFETY ANALYSES

The minimum required SDM is assumed as an initial condition in safety analysis. The safety analysis (Ref. 2) establishes an SDM that ensures specified acceptable fuel design limits are not exceeded for normal operation and AOOs, with the assumption of the highest worth CEA stuck out following a reactor trip. For MODE 5, the primary safety analysis that relies on the SDM limits is the boron dilution analysis.

BASES

APPLICABLE SAFETY ANALYSES (continued)

The acceptance criteria for the SDM are that specified acceptable fuel design limits are maintained. This is done by ensuring that:

a. The reactor can be made subcritical from all operating conditions, transients, and Design Basis Events,

b. The reactivity transients associated with postulated accident conditions are controllable within acceptable limits (departure from nucleate boiling ratio (DNBR), fuel centerline temperature limit AOOs, and ≤ 280 cal/gm energy deposition for the CEA ejection accident), and

c. The reactor will be maintained sufficiently subcritical to preclude inadvertent criticality in the shutdown condition.

The most limiting accident for the SDM requirements are based on a main steam line break (MSLB), as described in the accident analysis (Ref. 2). The increased steam flow resulting from a pipe break in the main steam system causes an increased energy removal from the affected steam generator (SG), and consequently the RCS. This results in a reduction of the reactor coolant temperature. The resultant coolant shrinkage causes a reduction in pressure. In the presence of a negative moderator temperature coefficient, this cooldown causes an increase in core reactivity. As RCS temperature decreases, the severity of an MSLB decreases until the MODE 5 value is reached. The most limiting MSLB, with respect to potential fuel damage before a reactor trip occurs, is a guillotine break of a main steam line inside containment initiated at the end of core life. The positive reactivity addition from the moderator temperature decrease will terminate when the affected SG boils dry, thus terminating RCS heat removal and cooldown. Following the MSLB, a post trip return to power may occur; however, no fuel damage occurs as a result of the post trip return to power, and THERMAL POWER does not violate the Safety Limit (SL) requirement of SL 2.1.1.

In addition to the limiting MSLB transient, the SDM requirement for MODES 3 and 4 must also protect against:

a. Inadvertent boron dilution,

b. An uncontrolled CEA withdrawal from a subcritical condition,

c. Startup of an inactive reactor coolant pump (RCP), and

d. CEA ejection.

BASES

APPLICABLE SAFETY ANALYSES (continued)

Each of these is discussed below.

In the boron dilution analysis, the required SDM defines the reactivity difference between an initial subcritical boron concentration and the corresponding critical boron concentration. These values, in conjunction with the configuration of the RCS and the assumed dilution flow rate, directly affect the results of the analysis. This event is most limiting at the beginning of core life when critical boron concentrations are highest.

The withdrawal of CEAs from subcritical conditions adds reactivity to the reactor core, causing both the core power level and heat flux to increase with corresponding increases in reactor coolant temperatures and pressure. The withdrawal of CEAs also produces a time dependent redistribution of core power.

Depending on the system initial conditions and reactivity insertion rate, the uncontrolled CEA withdrawal transient is terminated by either a high power level trip or a high pressurizer pressure trip. In all cases, power level, RCS pressure, linear heat rate, and the DNBR do not exceed allowable limits.

The startup of an inactive RCP will not result in a "cold water" criticality, even if the maximum difference in temperature exists between the SG and the core. The maximum positive reactivity addition that can occur due to an inadvertent RCP start is less than half the minimum required SDM. An idle RCP cannot, therefore, produce a return to power from the hot standby condition.

The withdrawal of CEAs from subcritical or low power Conditions adds reactivity to the reactor core, causing both the core power level and heat flux to increase with corresponding increases in reactor coolant temperatures and pressure. The withdrawal of CEAs also produces a time dependent redistribution of core power.

The SDM satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

The MSLB (Ref. 2) and the boron dilution (Ref. 3) accidents are the most limiting analyses that establish the SDM value of the LCO. For MSLB accidents, if the LCO is violated, there is a potential to exceed the DNBR limit and to exceed 10 CFR 100, "Reactor Site Criterion," limits (Ref. 4). For the boron dilution accident, if the LCO is violated, then the minimum required time assumed for operator action to terminate dilution may no longer be applicable.

BASES

LCO (continued)

SDM is a core physics design condition that can be ensured through CEA positioning (regulating and shutdown CEAs) and through the soluble boron concentration.

APPLICABILITY

In MODES 3, 4, and 5, the SDM requirements are applicable to provide sufficient negative reactivity to meet the assumptions of the safety analyses discussed above. In MODES 1 and 2, SDM is ensured by complying with LCO 3.1.5, "Shutdown Control Element Assembly (CEA) Insertion Limits," and LCO 3.1.6. In MODE 6, the shutdown reactivity requirements are given in LCO 3.9.1, "Boron Concentration."

ACTIONS

A.1

If the SDM requirements are not met, boration must be initiated promptly. A Completion Time of 15 minutes is adequate for an operator to correctly align and start the required systems and components. It is assumed that boration will be continued until the SDM requirements are met.

In the determination of the required combination of boration flow rate and boron concentration, there is no unique requirement that must be satisfied. Since it is imperative to raise the boron concentration of the RCS as soon as possible, the boron concentration should be a highly concentrated solution, such as that normally found in the boric acid storage tank or the borated water storage tank. The operator should borate with the best source available for the plant conditions.

In determining the boration flow rate, the time core life must be considered. For instance, the most difficult time in core life to increase the RCS boron concentration is at the beginning of cycle, when the boron concentration may approach or exceed 2000 ppm. Assuming that a value of 1% $\Delta k/k$ must be recovered and a boration flow rate of [ ] gpm, it is possible to increase the boron concentration of the RCS by 100 ppm in approximately 35 minutes. If a boron worth of 10 pcm/ppm is assumed, this combination of parameters will increase the SDM by 1% $\Delta k/k$. These boration parameters of [ ] gpm and [ ] ppm represent typical values and are provided for the purpose of offering a specific example.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.1.1.1

SDM is verified by performing a reactivity balance calculation, considering the listed reactivity effects:

a. RCS boron concentration,

b. CEA positions,

c. RCS average temperature,

d. Fuel burnup based on gross thermal energy generation,

e. Xenon concentration,

f. Samarium concentration, and

g. Isothermal temperature coefficient (ITC).

Using the ITC accounts for Doppler reactivity in this calculation because the reactor is subcritical, and the fuel temperature will be changing at the same rate as the RCS.

The Frequency of 24 hours is based on the generally slow change in required boron concentration, and also allows sufficient time for the operator to collect the required data, which includes performing a boron concentration analysis, and complete the calculation.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 26.

2. FSAR, Section [15.4.2].

3. FSAR, Section [15.4.2].

4. 10 CFR 100.

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.2 Reactivity Balance (Digital)

BASES

BACKGROUND

According to GDC 26, GDC 28, and GDC 29 (Ref. 1), reactivity shall be controllable, such that, subcriticality is maintained under cold conditions, and acceptable fuel design limits are not exceeded during normal operation and anticipated operational occurrences. Therefore, reactivity balance is used as a measure of the predicted versus measured core reactivity during power operation. The periodic confirmation of core reactivity is necessary to ensure that Design Basis Accident (DBA) and transient safety analyses remain valid. A large reactivity difference could be the result of unanticipated changes in fuel, control element assembly (CEA) worth, or operation at Conditions not consistent with those assumed in the predictions of core reactivity, and could potentially result in a loss of SDM or violation of acceptable fuel design limits. Comparing predicted versus measured core reactivity validates the nuclear methods used in the safety analysis and supports the SDM demonstrations (LCO 3.1.1, "SHUTDOWN MARGIN (SDM)") in ensuring the reactor can be brought safely to cold, subcritical conditions.

When the reactor core is critical or in normal power operation, a reactivity balance exists and the net reactivity is zero. A comparison of predicted and measured reactivity is convenient under such a balance, since parameters are being maintained relatively stable under steady state power conditions. The positive reactivity inherent in the core design is balanced by the negative reactivity of the control components, thermal feedback, neutron leakage, and materials in the core that absorb neutrons, such as burnable absorbers producing zero net reactivity. Excess reactivity can be inferred from the critical boron curve, which provides an indication of the soluble boron concentration in the Reactor Coolant System (RCS) versus cycle burnup. Periodic measurement of the RCS boron concentration for comparison with the predicted value with other variables fixed (such as CEA height, temperature, pressure, and power) provides a convenient method of ensuring that core reactivity is within design expectations, and that the calculational models used to generate the safety analysis are adequate.

In order to achieve the required fuel cycle energy output, the uranium enrichment in the new fuel loading and in the fuel remaining from the previous cycle, provides excess positive reactivity beyond that required to sustain steady state operation throughout the cycle. When the reactor is critical at RTP and moderator temperature, the excess positive reactivity is compensated by burnable absorbers (if any), CEAs, whatever neutron poisons (mainly xenon and samarium) are present in the fuel, and the RCS boron concentration.

BASES

BACKGROUND (continued)

When the core is producing THERMAL POWER, the fuel is being depleted and excess reactivity is decreasing. As the fuel depletes, the RCS boron concentration is reduced to decrease negative reactivity and maintain constant THERMAL POWER. The critical boron curve is based on steady state operation at RTP. Therefore, deviations from the predicted boron letdown curve may indicate deficiencies in the design analysis, deficiencies in the calculational models, or abnormal core conditions, and must be evaluated.

APPLICABLE SAFETY ANALYSES

Accurate prediction of core reactivity is either an explicit or implicit assumption in the accident analysis evaluations. Every accident evaluation (Ref. 2) is, therefore, dependent upon accurate evaluation of core reactivity. In particular, SDM, and reactivity transients such as CEA withdrawal accidents or CEA ejection accidents, are very sensitive to accurate prediction of core reactivity. These accident analysis evaluations rely on computer codes that have been qualified against available test data, operating plant data, and analytical benchmarks. Monitoring reactivity balance additionally ensures that the nuclear methods provide an accurate representation of the core reactivity.

Design calculations and safety analyses are performed for each fuel cycle for the purpose of predetermining reactivity behavior and the RCS boron concentration requirements for reactivity control during fuel depletion.

The comparison between measured and predicted initial core reactivity provides a normalization for calculational models used to predict core reactivity. If the measured and predicted RCS boron concentrations for identical core conditions at beginning of cycle (BOC) do not agree, then the assumptions used in the reload cycle design analysis or the calculational models used to predict soluble boron requirements may not be accurate. If reasonable agreement between measured and predicted core reactivity exists at BOC, then the prediction may be normalized to the measured boron concentration. Thereafter, any significant deviations in the measured boron concentration from the predicted critical boron curve that develop during fuel depletion may be an indication that the calculational model is not adequate for core burnups beyond BOC, or that an unexpected change in core conditions has occurred.

BASES

APPLICABLE SAFETY ANALYSES (continued)

The normalization of predicted RCS boron concentration to the measured value is typically performed after reaching RTP following startup from a refueling outage, with the CEAs in their normal positions for power operation. The normalization is performed at BOC conditions, so that core reactivity relative to predicted values can be continually monitored and evaluated as core conditions change during the cycle.

The reactivity balance satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

The reactivity balance limit is established to ensure plant operation is maintained within the assumptions of the safety analyses. Large differences between actual and predicted core reactivity may indicate that the assumptions of the DBA and transient analyses are no longer valid, or that the uncertainties in the nuclear design methodology are larger than expected. A limit on the reactivity balance of ± 1% $\Delta k/k$ has been established, based on engineering judgment. A 1% deviation in reactivity from that predicted is larger than expected for normal operation, and should therefore be evaluated.

When measured core reactivity is within 1% $\Delta k/k$ of the predicted value at steady state thermal conditions, the core is considered to be operating within acceptable design limits. Since deviations from the limit are normally detected by comparing predicted and measured steady state RCS critical boron concentrations, the difference between measured and predicted values would be approximately 100 ppm (depending on the boron worth) before the limit is reached. These values are well within the uncertainty limits for analysis of boron concentration samples, so that spurious violations of the limit due to uncertainty in measuring the RCS boron concentration are unlikely.

APPLICABILITY

The limits on core reactivity must be maintained during MODES 1 and 2 because a reactivity balance must exist when the reactor is critical or producing THERMAL POWER. As the fuel depletes, core conditions are changing, and confirmation of the reactivity balance ensures the core is operating as designed. This Specification does not apply in MODES 3, 4, and 5 because the reactor is shut down and the reactivity balance is not changing.

In MODE 6, fuel loading results in a continually changing core reactivity. Boron concentration requirements (LCO 3.9.1, "Boron Concentration") ensure that fuel movements are performed within the bounds of the safety analysis. An SDM demonstration is required during the first startup following operations that could have altered core reactivity (e.g., fuel movement, or CEA replacement, or shuffling).

BASES

ACTIONS

A.1 and A.2

Should an anomaly develop between measured and predicted core reactivity, an evaluation of the core design and safety analysis must be performed. Core conditions are evaluated to determine their consistency with input to design calculations. Measured core and process parameters are evaluated to determine that they are within the bounds of the safety analysis, and safety analysis calculational models are reviewed to verify that they are adequate for representation of the core conditions. The required Completion Time of 7 days is based on the low probability of a DBA occurring during this period, and allows sufficient time to assess the physical condition of the reactor and complete the evaluation of the core design and safety analysis.

Following evaluations of the core design and safety analysis, the cause of the reactivity anomaly may be resolved. If the cause of the reactivity anomaly is a mismatch in core conditions at the time of RCS boron concentration sampling, then a recalculation of the RCS boron concentration requirements may be performed to demonstrate that core reactivity is behaving as expected. If an unexpected physical change in the condition of the core has occurred, it must be evaluated and corrected, if possible. If the cause of the reactivity anomaly is in the calculation technique, then the calculational models must be revised to provide more accurate predictions. If any of these results are demonstrated and it is concluded that the reactor core is acceptable for continued operation, then the boron letdown curve may be renormalized, and power operation may continue. If operational restrictions or additional SRs are necessary to ensure the reactor core is acceptable for continued operation, then they must be defined.

The required Completion Time of 7 days is adequate for preparing whatever operating restrictions or Surveillances that may be required to allow continued reactor operation.

B.1

If the core reactivity cannot be restored to within the 1% $\Delta k/k$, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours. If the SDM for MODE 3 is not met, then boration required by SR 3.1.1.1 would occur. The allowed Completion Time is reasonable, based on operating experience, for reaching MODE 3 from full power conditions in an orderly manner and without challenging plant systems.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.1.2.1

Core reactivity is verified by periodic comparisons of measured and predicted RCS boron concentrations. The comparison is made considering that other core conditions are fixed or stable including CEA position, moderator temperature, fuel temperature, fuel depletion, xenon concentration, and samarium concentration. The Surveillance is performed prior to entering MODE 1 as an initial check on core conditions and design calculations at BOC. The SR is modified by three Notes. The first Note indicates that the normalization of predicted core reactivity to the measured value must take place within the first 60 effective full power days (EFPD) after each fuel loading. This allows sufficient time for core conditions to reach steady state, but prevents operation for a large fraction of the fuel cycle without establishing a benchmark for the design calculations. The required subsequent Frequency of 31 EFPD, following the initial 60 EFPD after entering MODE 1, is acceptable, based on the slow rate of core changes due to fuel depletion and the presence of other indicators (e.g., QPTR) for prompt indication of an anomaly. A Note, "only required after 60 EFPD," is added to the Frequency column to allow this. Another Note indicates that the performance of SR 3.1.2.1 is not required prior to entering MODE 2. This Note is required to allow a MODE 2 entry to verify core reactivity because Applicability is for MODES 1 and 2.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 26, GDC 28, and GDC 29.

2. FSAR, Section [ ].

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.3 Moderator Temperature Coefficient (MTC) (Digital)

BASES

BACKGROUND

According to GDC 11 (Ref. 1), the reactor core and its interaction with the Reactor Coolant System (RCS) must be designed for inherently stable power operation, even in the possible event of an accident. In particular, the net reactivity feedback in the system must compensate for any unintended reactivity increases.

The MTC relates a change in core reactivity to a change in reactor coolant temperature. A positive MTC means that reactivity increases with increasing moderator temperature; conversely, a negative MTC means that reactivity decreases with increasing moderator temperature. The reactor is designed to operate with a negative MTC over the largest possible range of fuel cycle operation. Therefore, a coolant temperature increase will cause a reactivity decrease, so that the coolant temperature tends to return toward its initial value. Reactivity increases that cause a coolant temperature increase will thus be self limiting, and stable power operation will result. The same characteristic is true when the MTC is positive and coolant temperature decreases occur.

MTC values are predicted at selected burnups during the safety evaluation analysis and are confirmed to be acceptable by measurements. Both initial and reload cores are designed so that the beginning of cycle (BOC) MTC is less positive than that allowed by the LCO. The actual value of the MTC is dependent on core characteristics such as fuel loading and reactor coolant soluble boron concentration. The core design may require additional fixed distributed poisons (lumped burnable poison assemblies) to yield an MTC at the BOC within the range analyzed in the plant accident analysis. The end of cycle (EOC) MTC is also limited by the requirements of the accident analysis. Fuel cycles that are designed to achieve high burnups or that have changes to other characteristics are evaluated to ensure that the MTC does not exceed the EOC limit.

APPLICABLE SAFETY ANALYSES

The acceptance criteria for the specified MTC are:

a. The MTC values must remain within the bounds of those used in the accident analysis (Ref. 2) and

b. The MTC must be such that inherently stable power operations result during normal operation and during accidents, such as overheating and overcooling events.

BASES

APPLICABLE SAFETY ANALYSES (continued)

Reference 2 contains analyses of accidents that result in both overheating and overcooling of the reactor core. MTC is one of the controlling parameters for core reactivity in these accidents. Both the most positive value and most negative value of the MTC are important to safety, and both values must be bounded. Values used in the analyses consider worst case conditions, such as very large soluble boron concentrations, to ensure the accident results are bounding (Ref. 3).

Accidents that cause core overheating, either by decreased heat removal or increased power production, must be evaluated for results when the MTC is positive. Reactivity accidents that cause increased power production include the control element assembly (CEA) withdrawal transient from either zero or full THERMAL POWER. The limiting overheating event relative to plant response is based on the maximum difference between core power and steam generator heat removal during a transient. The most limiting event with respect to a positive MTC is a CEA withdrawal accident from zero power, also referred to as a startup accident (Ref. 4).

Accidents that cause core overcooling must be evaluated for results when the MTC is most negative. The event that produces the most rapid cooldown of the RCS, and is therefore the most limiting event with respect to the negative MTC, is a steam line break (SLB) event. Following the reactor trip for the postulated EOC SLB event, the large moderator temperature reduction combined with the large negative MTC may produce reactivity increases that are as much as the shutdown reactivity. When this occurs, a substantial fraction of core power is produced with all CEAs inserted, except the most reactive one, which is assumed withdrawn. Even if the reactivity increase produces slightly subcritical conditions, a large fraction of core power may be produced through the effects of subcritical neutron multiplication.

MTC values are bounded in reload safety evaluations assuming steady state conditions at BOC and EOC. A middle of cycle (MOC) measurement is conducted at conditions when the RCS boron concentration reaches approximately 300 ppm. The measured value may be extrapolated to project the EOC value, in order to confirm reload design predictions.

The MTC satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO

LCO 3.1.3 requires the MTC to be within the specified limits of the COLR to ensure the core operates within the assumptions of the accident analysis. During the reload core safety evaluation, the MTC is analyzed to determine that its values remain within the bounds of the original accident analysis during operation. The limit on a positive MTC ensures that core overheating accidents will not violate the accident analysis assumptions. The negative MTC limit for EOC specified in the COLR ensures that core overcooling accidents will not violate the accident analysis assumptions.

MTC is a core physics parameter determined by the fuel and fuel cycle design and cannot be easily controlled once the core design is fixed. During operation, therefore, the LCO can only be ensured through measurement. The surveillance checks at BOC and MOC on an MTC provide confirmation that the MTC is behaving as anticipated, so that the acceptance criteria are met.

APPLICABILITY

In MODE 1, the limits on the MTC must be maintained to ensure that any accident initiated from THERMAL POWER operation will not violate the design assumptions of the accident analysis. In MODE 2, the limits must also be maintained to ensure startup and subcritical accidents, such as the uncontrolled CEA assembly or group withdrawal, will not violate the assumptions of the accident analysis. In MODES 3, 4, 5, and 6, this LCO is not applicable, since no Design Basis Accidents (DBAs) using the MTC as an analysis assumption are initiated from these MODES. However, the variation of the MTC, with temperature in MODES 3, 4, and 5, for DBAs initiated in MODES 1 and 2, is accounted for in the subject accident analysis. The variation of the MTC, with temperature assumed in the safety analysis, is accepted as valid once the BOC and MOC measurements are used for normalization.

ACTIONS

A.1

MTC is a function of the fuel and fuel cycle designs, and cannot be controlled directly once the designs have been implemented in the core. If MTC exceeds its limits, the reactor must be placed in MODE 3. This eliminates the potential for violation of the accident analysis bounds. The associated Completion Time of 6 hours is reasonable, considering the probability of an accident occurring during the time period that would require an MTC value within the LCO limits, and the time for reaching MODE 3 from full power conditions in an orderly manner and without challenging plant systems.

BASES

SURVEILLANCE REQUIREMENTS	SR 3.1.3.1 and SR 3.1.3.2 The SRs for measurement of the MTC at the beginning and middle of each fuel cycle provide for confirmation of the limiting MTC values. The MTC changes smoothly from most positive (least negative) to most negative value during fuel cycle operation, as the RCS boron concentration is reduced to compensate for fuel depletion. The requirement for measurement prior to operation > 5% RTP satisfies the confirmatory check on the most positive (least negative) MTC value. The requirement for measurement, within 7 days after reaching 40 effective full power days and a 2/3 core burnup, satisfies the confirmatory check of the most negative MTC value. The measurement is performed at any THERMAL POWER so that the projected EOC MTC may be evaluated before the reactor actually reaches the EOC condition. MTC values may be extrapolated and compensated to permit direct comparison to the specified MTC limits. SR 3.1.3.2 is modified by a Note, which indicates that if extrapolated MTC is more negative than the EOC COLR limit, the Surveillance may be repeated, and that shutdown must occur prior to exceeding the minimum allowable boron concentration at which MTC is projected to exceed the lower limit. An engineering evaluation is performed if the extrapolated value of MTC exceeds the Specification limits.
REFERENCES	1. 10 CFR 50, Appendix A, GDC 11. 2. FSAR, Section [ ]. 3. FSAR, Section [ ]. 4. FSAR, Section [ ].

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.4 Control Element Assembly (CEA) Alignment (Digital)

BASES

BACKGROUND

The OPERABILITY (i.e., trippability) of the shutdown and regulating Control Element Assemblies (CEAs) is an initial assumption in all safety analyses that assume CEA insertion upon reactor trip. Maximum CEA misalignment is an initial assumption in the safety analyses that directly affects core power distributions and assumptions of available SDM.

The applicable criteria for these reactivity and power distribution design requirements are 10 CFR 50, Appendix A, GDC 10 and GDC 26 (Ref. 1) and 10 CFR 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Cooled Nuclear Power Plants" (Ref. 2).

Mechanical or electrical failures may cause a CEA to become inoperable or to become misaligned from its group. CEA inoperability or misalignment may cause increased power peaking, due to the asymmetric reactivity distribution and a reduction in the total available CEA worth for reactor shutdown. Therefore, CEA alignment and operability are related to core operation in design power peaking limits and the core design requirement of a minimum SDM.

Limits on CEA alignment and OPERABILITY have been established, and all CEA positions are monitored and controlled during power operation to ensure that the power distribution and reactivity limits defined by the design power peaking and SDM limits are preserved.

CEAs are moved by their control element drive mechanisms (CEDMs). Each CEDM moves its CEA one step (approximately ¾ inch) at a time, but at varying rates (steps per minute) depending on the signal output from the Control Element Drive Mechanism Control System (CEDMCS).

The CEAs are arranged into groups that are radially symmetric. Therefore, movement of the CEAs does not introduce radial asymmetries in the core power distribution. The shutdown and regulating CEAs provide the required reactivity worth for immediate reactor shutdown upon a reactor trip. The regulating CEAs also provide reactivity (power level) control during normal operation and transients. Their movement may be automatically controlled by the Reactor Regulating System. Part length CEAs are not credited in the safety analyses for shutting down the reactor, as are the regulating and shutdown groups. The part length CEAs are used solely for ASI control.

BASES

BACKGROUND (continued)

The axial position of shutdown and regulating CEAs is indicated by two separate and independent systems, which are the Plant Computer CEA Position Indication System and the Reed Switch Position Indication System.

The Plant Computer CEA Position Indication System counts the commands sent to the CEA gripper coils from the CEDMCS that moves the CEAs. There is one step counter for each group of CEAs. Individual CEAs in a group all receive the same signal to move and should, therefore, all be at the same position indicated by the group step counter for that group. The Plant Computer CEA Position Indication System is considered highly precise (± one step or ± ¾ inch). If a CEA does not move one step for each command signal, the step counter will still count the command and incorrectly reflect the position of the CEA.

The Reed Switch Position Indication System provides a highly accurate indication of actual CEA position, but at a lower precision than the step counters. This system is based on inductive analog signals from a series of reed switches spaced along a tube with a center to center distance of 1.5 inches, which is two steps. To increase the reliability of the system, there are redundant reed switches at each position.

APPLICABLE SAFETY ANALYSES

CEA misalignment accidents are analyzed in the safety analysis (Ref. 3). The accident analysis defines CEA misoperation as any event, with the exception of sequential group withdrawals, which could result from a single malfunction in the reactivity control systems. For example, CEA misalignment may be caused by a malfunction of the CEDM, CEDMCS, or by operator error. A stuck CEA may be caused by mechanical jamming of the CEA fingers or of the gripper. Inadvertent withdrawal of a single CEA may be caused by opening of the electrical circuit of the CEDM holding coil for a full length or part length CEA. A dropped CEA subgroup could be caused by an electrical failure in the CEA coil power programmers.

The acceptance criteria for addressing CEA inoperability or misalignment are that:

a. There shall be no violations of either:

    1. Specified acceptable fuel design limits or

    2. Reactor Coolant System (RCS) pressure boundary integrity and

b. The core must remain subcritical after accident transients.

BASES

APPLICABLE SAFETY ANALYSES (continued)

Three types of misalignment are distinguished. During movement of a group, one CEA may stop moving while the other CEAs in the group continue. This condition may cause excessive power peaking. The second type of misalignment occurs if one CEA fails to insert upon a reactor trip and remains stuck fully withdrawn. This condition requires an evaluation to determine that sufficient reactivity worth is held in the remaining CEAs to meet the SDM requirement with the maximum worth CEA stuck fully withdrawn. If a CEA is stuck in the fully withdrawn position, its worth is added to the SDM requirement, since the safety analysis does not take two stuck CEAs into account. The third type of misalignment occurs when one CEA drops partially or fully into the reactor core. This event causes an initial power reduction followed by a return towards the original power due to positive reactivity feedback from the negative moderator temperature coefficient. Increased peaking during the power increase may result in excessive local linear heat rates (LHRs).

Two types of analyses are performed in regard to static CEA misalignment (Ref. 4). With CEA banks at their insertion limits, one type of analysis considers the case when any one CEA is inserted [ ] inches into the core. The second type of analysis considers the case of a single CEA withdrawn [ ] inches from a bank inserted to its insertion limit. Satisfying limits on departure from nucleate boiling ratio (DNBR) in both of these cases bounds the situation when a CEA is misaligned from its group by [7 inches].

Another type of misalignment occurs if one CEA fails to insert upon a reactor trip and remains stuck fully withdrawn. This condition is assumed in the evaluation to determine that the required SDM is met with the maximum worth CEA also fully withdrawn (Ref. 5).

The effect of any misoperated CEA on the core power distribution will be assessed by the CEA calculators, and an appropriately augmented power distribution penalty factor will be supplied as input to the core protection calculators (CPCs). As the reactor core responds to the reactivity changes caused by the misoperated CEA and the ensuing reactor coolant and Doppler feedback effects, the CPCs will initiate a low DNBR or high local power density trip signal if specified acceptable fuel design limits (SAFDLs) are approached.

BASES

APPLICABLE SAFETY ANALYSES (continued)

Since the CEA drop incidents result in the most rapid approach to SAFDLs caused by a CEA misoperation, the accident analysis analyzed a single full length CEA drop, a single part length CEA drop, and a part length CEA subgroup drop. The most rapid approach to the DNBR SAFDL may be caused by either a single full length drop or a part length CEA subgroup drop depending upon initial conditions. The most rapid approach to the fuel centerline melt SAFDL is caused by a single part length CEA drop.

In the case of the full length CEA drop, a prompt decrease in core average power and a distortion in radial power are initially produced, which when conservatively coupled result in local power and heat flux increases, and a decrease in DNBR. For plant operation within the DNBR and local power density (LPD) LCOs, DNBR and LPD trips can normally be avoided on a dropped CEA.

For a part length CEA subgroup drop, a distortion in power distribution, and a decrease in core power are produced. As the dropped part length CEA subgroup is detected, an appropriate power distribution penalty factor is supplied to the CPCs, and a reactor trip signal on low DNBR is generated. For the part length CEA drop, both core average power and three dimensional peak to average power density increase promptly. As the dropped part length CEA is detected, core power and an appropriately augmented power distribution penalty factor are supplied to the CPCs.

CEA alignment limits and OPERABILITY requirements satisfy Criteria 2 and 3 of 10 CFR 50.36(c)(2)(ii).

LCO

The limits on shutdown and regulating CEA alignments ensure that the assumptions in the safety analysis will remain valid. The requirements on CEA OPERABILITY ensure that upon reactor trip, the CEAs will be available and will be inserted to provide enough negative reactivity to shut down the reactor. The CEA OPERABILITY requirements (i.e., trippability) are separate from the alignment requirements which ensure that the CEA banks maintain the correct power distribution and CEA alignment. The CEA OPERABILITY requirement is satisfied provided the CEA will fully insert in the required CEA drop time assumed in the safety analysis. CEA control malfunctions that result in the inability to move a CEA (e.g., CEA lift coil failures), but that do not impact trippability, do not result in CEA inoperability.

BASES

LCO (continued)

The requirement is to maintain the CEA alignment to within [7 inches] between any CEA and its group. The minimum misalignment assumed in safety analysis is [19 inches], and in some cases, a total misalignment from fully withdrawn to fully inserted is assumed.

Failure to meet the requirements of this LCO may produce unacceptable power peaking factors and LHRs, or unacceptable SDMs, all of which may constitute initial conditions inconsistent with the safety analysis.

APPLICABILITY

The requirements on CEA OPERABILITY and alignment are applicable in MODES 1 and 2 because these are the only MODES in which neutron (or fission) power is generated, and the OPERABILITY (i.e., trippability) and alignment of CEAs have the potential to affect the safety of the plant. In MODES 3, 4, 5, and 6, the alignment limits do not apply because the CEAs are bottomed, and the reactor is shut down and not producing fission power. In the shutdown modes, the OPERABILITY of the shutdown and regulating CEAs has the potential to affect the required SDM, but this effect can be compensated for by an increase in the boron concentration of the RCS. See LCO 3.1.1, "SHUTDOWN MARGIN (SDM)," for SDM in MODES 3, 4, and 5, and LCO 3.9.1, "Boron Concentration," for boron concentration requirements during refueling.

ACTIONS

<u>A.1 and A.2</u>

If one or more CEAs (regulating, shutdown or part length) are misaligned by [7 inches] and ≤ [19 inches], or one CEA misaligned by > [19 inches], continued operation in MODES 1 and 2 may continue, provided, within 1 hour, the power is reduced in accordance with Figure 3.1.4-1, and within 2 hours CEA alignment is restored.

Regulating and part length CEA alignment can be restored by either aligning the misaligned CEA(s) to within [7 inches] of its group or aligning the misaligned CEA's group to within [7 inches] of the misaligned CEA. Shutdown CEA alignment can be restored by aligning the misaligned CEA(s) to within [7 inches] of its group.

Xenon redistribution in the core starts to occur as soon as a CEA becomes misaligned. Reducing THERMAL POWER in accordance with Figure 3.1.4-1 (in the accompanying LCO) ensures acceptable power distributions are maintained (Ref. 6). For small misalignments (< [19 inches]) of the CEAs, there is:

BASES

ACTIONS (continued)

a. A small effect on the time dependent long term power distributions relative to those used in generating LCOs and limiting safety system settings (LSSS) setpoints,

b. A negligible effect on the available SDM, and

c. A small effect on the ejected CEA worth used in the accident analysis.

With a large CEA misalignment (≥ [19 inches]), however, this misalignment would cause distortion of the core power distribution. This distortion may, in turn, have a significant effect on the time dependent, long term power distributions relative to those used in generating LCOs and LSSS setpoints. The effect on the available SDM and the ejected CEA worth used in the accident analysis remain small. Therefore, this condition is limited to the single CEA misalignment, while still allowing 2 hours for recovery. In both cases, a 2 hour time period is sufficient to:

a. Identify cause of a misaligned CEA,

b. Take appropriate corrective action to realign the CEAs, and

c. Minimize the effects of xenon redistribution.

The CEA must be returned to OPERABLE status within 2 hours or transition to MODE 3.

B.1

If a Required Action or associated Completion Time of Condition A is not met, one or more full length CEAs are inoperable, or two or more CEAs are misaligned by > [19 inches], the unit is required to be brought to MODE 3. By being brought to MODE 3, the unit is brought outside its MODE of applicability. This is because these cases are indicative of a loss of SDM and power distribution, and a loss of safety function, respectively.

When a Required Action cannot be completed within the required Completion Time, a controlled shutdown should be commenced. The allowed Completion Time of 6 hours is reasonable, based on operating experience, for reaching MODE 3 from full power conditions in an orderly manner and without challenging plant systems.

BASES

ACTIONS (continued)

Continued operation is not allowed in the case of more than one CEA(s) misaligned from any other CEA in its group by > [19 inches], or with one or more full length CEAs inoperable

SURVEILLANCE REQUIREMENTS

SR 3.1.4.1

Verification that individual CEA positions are within [7 inches] (indicated reed switch positions) of all other CEAs in the group at a 12 hour Frequency allows the operator to detect a CEA that is beginning to deviate from its expected position. The specified Frequency takes into account other CEA position information that is continuously available to the operator in the control room, so that during actual CEA motion, deviations can immediately be detected.

SR 3.1.4.2

OPERABILITY of at least two CEA position indicator channels is required to determine CEA positions, and thereby ensure compliance with the CEA alignment and insertion limits. The CEA full in and full out limits provide an additional independent means for determining the CEA positions when the CEAs are at either their fully inserted or fully withdrawn positions.

SR 3.1.4.3

Verifying each full length CEA is trippable would require that each CEA be tripped. In MODES 1 and 2 tripping each full length CEA would result in radial or axial power tilts, or oscillations. Therefore individual full length CEAs are exercised every 92 days to provide increased confidence that all full length CEAs continue to be trippable, even if they are not regularly tripped. A movement of [5 inches] is adequate to demonstrate motion without exceeding the alignment limit when only one full length CEA is being moved. The 92 day Frequency takes into consideration other information available to the operator in the control room and other surveillances being performed more frequently, which add to the determination of OPERABILITY of the CEAs (Ref. 7). Between required performances of SR 3.1.4.3, if a CEA(s) is discovered to be immovable, the CEA is considered to be OPERABLE. At anytime, if a CEA(s) is immovable, a determination of the trippability (OPERABILITY) of that CEA(s) must be made, and appropriate action taken.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.1.4.4

Performance of a CHANNEL FUNCTIONAL TEST of each reed switch position transmitter channel ensures the channel is OPERABLE and capable of indicating CEA position. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions. Since this test must be performed when the reactor is shut down, an 18 month Frequency to be coincident with refueling outage was selected. Operating experience has shown that these components usually pass this Surveillance when performed at a Frequency of once every 18 months. Therefore, the Frequency was concluded to be acceptable from a reliability standpoint.

SR 3.1.4.5

Verification of full length CEA drop times determines that the maximum CEA drop time permitted is consistent with the assumed drop time used in the safety analysis (Ref. 7). Measuring drop times prior to reactor criticality, after reactor vessel head removal, ensures the reactor internals and CEDM will not interfere with CEA motion or drop time, and that no degradation in these systems has occurred that would adversely affect CEA motion or drop time. Individual CEAs whose drop times are greater than safety analysis assumptions are not OPERABLE. This SR is performed prior to criticality due to the plant conditions needed to perform the SR and the potential for an unplanned plant transient if the Surveillance were performed with the reactor at power.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 10 and GDC 26.
2. 10 CFR 50.46.
3. FSAR, Section [ ].
4. FSAR, Section [ ].

BASES

REFERENCES (continued)

5. FSAR, Section [ ].

6. FSAR, Section [ ].

7. FSAR, Section [ ].

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.5 Shutdown Control Element Assembly (CEA) Insertion Limits (Digital)

BASES

BACKGROUND

The insertion limits of the shutdown Control Element Assemblies (CEAs) are initial assumptions in all safety analyses that assume CEA insertion upon reactor trip. The insertion limits directly affect core power distributions and assumptions of available SDM, ejected CEA worth, and initial reactivity insertion rate.

The applicable criteria for these reactivity and power distribution design requirements are 10 CFR 50, Appendix A, GDC 10, "Reactor Design," and GDC 26, "Reactivity Limits" (Ref. 1), and 10 CFR 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Nuclear Power Reactors" (Ref. 2). Limits on shutdown CEA insertion have been established, and all CEA positions are monitored and controlled during power operation to ensure that the reactivity limits, ejected CEA worth, and SDM limits are preserved.

The shutdown CEAs are arranged into groups that are radially symmetric. Therefore, movement of the shutdown CEAs does not introduce radial asymmetries in the core power distribution. The shutdown and regulating CEAs provide the required reactivity worth for immediate reactor shutdown upon a reactor trip.

The design calculations are performed with the assumption that the shutdown CEAs are withdrawn prior to the regulating CEAS. The shutdown CEAs can be fully withdrawn without the core going critical. This provides available negative reactivity for SDM in the event of boration errors. The shutdown CEAs are controlled manually or automatically by the control room operator. During normal unit operation, the shutdown CEAs are fully withdrawn. The shutdown CEAs must be completely withdrawn from the core prior to withdrawing regulating CEAs during an approach to criticality. The shutdown CEAs are then left in this position until the reactor is shut down. They affect core power, burnup distribution, and add negative reactivity to shut down the reactor upon receipt of a reactor trip signal.

APPLICABLE SAFETY ANALYSES

Accident analysis assumes that the shutdown CEAs are fully withdrawn any time the reactor is critical. This ensures that:

a. The minimum SDM is maintained and

b. The potential effects of a CEA ejection accident are limited to acceptable limits.

BASES

APPLICABLE SAFETY ANALYSES (continued)

CEAs are considered fully withdrawn at 145 inches, since this position places them outside the active region of the core.

On a reactor trip, all CEAs (shutdown CEAs and regulating CEAs), except the most reactive CEA, are assumed to insert into the core. The shutdown and regulating CEAs shall be at their insertion limits and available to insert the maximum amount of negative reactivity on a reactor trip signal. The regulating CEAs may be partially inserted in the core as allowed by LCO 3.1.6, "Regulating Control Element Assembly (CEA) Insertion Limits." The shutdown CEA insertion limit is established to ensure that a sufficient amount of negative reactivity is available to shut down the reactor and maintain the required SDM (see LCO 3.1.1, "SHUTDOWN MARGIN (SDM)") following a reactor trip from full power. The combination of regulating CEAs and shutdown CEAs (less the most reactive CEA, which is assumed to be fully withdrawn) is sufficient to take the reactor from full power conditions at rated temperature to zero power, and to maintain the required SDM at rated no load temperature (Ref. 3). The shutdown CEA insertion limit also limits the reactivity worth of an ejected shutdown CEA.

The acceptance criteria for addressing shutdown CEA as well as regulating CEA insertion limits and inoperability or misalignment are that:

a. There be no violation of either:

    1. Specified acceptable fuel design limits or

    2. Reactor Coolant System pressure boundary damage integrity and

b. The core remains subcritical after accident transients.

The shutdown CEA insertion limits satisfy Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

The shutdown CEAs must be within their insertion limits any time the reactor is critical or approaching criticality. This ensures that a sufficient amount of negative reactivity is available to shut down the reactor and maintain the required SDM following a reactor trip.

BASES

APPLICABILITY

The shutdown CEAs must be within their insertion limits, with the reactor in MODES 1 and 2. The Applicability in MODE 2 begins any time any regulating CEA is not fully inserted. This ensures that a sufficient amount of negative reactivity is available to shut down the reactor and maintain the required SDM following a reactor trip. In MODE 3, 4, 5, or 6, the shutdown CEAs are fully inserted in the core and contribute to the SDM. Refer to LCO 3.1.1, "SHUTDOWN MARGIN (SDM)," for SDM requirements in MODES 3, 4, and 5. LCO 3.9.1, "Boron Concentration," ensures adequate SDM in MODE 6.

This LCO has been modified by a Note indicating the LCO requirement is suspended during SR 3.1.4.5, which verifies the freedom of the CEAs to move, and requires the shutdown CEAs to move below the LCO limits, which would normally violate the LCO.

ACTIONS

A.1

Prior to entering this Condition, the shutdown CEAs were fully withdrawn. If a shutdown CEA is then inserted into the core, its potential negative reactivity is added to the core as it is inserted.

If the CEA(s) is not restored to within limits within 1 hour, then an additional 1 hour is allowed for restoring the CEA(s) to within limits. The 2 hour total Completion Time allows the operator adequate time to adjust the CEA(s) in an orderly manner and is consistent with the required Completion Times in LCO 3.1.4, "Control Element Assembly (CEA) Alignment."

B.1

When Required Action A.1 or Required Action A.2 cannot be met or completed within the required Completion Time, a controlled shutdown should be commenced. The allowed Completion Time of 6 hours is reasonable, based on operating experience, for reaching MODE 3 from full power conditions in an orderly manner and without challenging plant systems.

BASES

SURVEILLANCE REQUIREMENTS	<u>SR 3.1.5.1</u> Verification that the shutdown CEAs are within their insertion limits prior to an approach to criticality ensures that when the reactor is critical, or being taken critical, the shutdown CEAs will be available to shut down the reactor, and the required SDM will be maintained following a reactor trip. This SR and Frequency ensure that the shutdown CEAs are withdrawn before the regulating CEAs are withdrawn during a unit startup. Since the shutdown CEAs are positioned manually by the control room operator, verification of shutdown CEA position at a Frequency of 12 hours is adequate to ensure that the shutdown CEAs are within their insertion limits. Also, the Frequency takes into account other information available to the operator in the control room for the purpose of monitoring the status of the shutdown CEAs.
REFERENCES	1. 10 CFR 50, Appendix A, GDC 10 and GDC 26. 2. 10 CFR 50.46. 3. FSAR, Section [ ].

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.6 Regulating Control Element Assembly (CEA) Insertion Limits (Digital)

BASES

BACKGROUND

The insertion limits of the regulating control element assemblies (CEAs) are initial assumptions in all safety analyses that assume CEA insertion upon reactor trip. The insertion limits directly affect core power distributions, assumptions of available SDM, and initial reactivity insertion rate. The applicable criteria for these reactivity and power distribution design requirements are 10 CFR 50, Appendix A, GDC 10, "Reactor Design," and GDC 26, "Reactivity Limits" (Ref. 1), and 10 CFR 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Nuclear Power Reactors" (Ref. 2).

Limits on regulating CEA insertion have been established, and all CEA positions are monitored and controlled during power operation to ensure that the power distribution and reactivity limits defined by the design power peaking, ejected CEA worth, reactivity insertion rate, and SDM limits are preserved.

The regulating CEA groups operate with a predetermined amount of position overlap, in order to approximate a linear relation between CEA worth and position (integral CEA worth). The regulating CEA groups are withdrawn and operate in a predetermined sequence. The group sequence and overlap limits are specified in the COLR.

The regulating CEAs are used for precise reactivity control of the reactor. The positions of the regulating CEAs are manually controlled. They are capable of adding reactivity very quickly (compared to borating or diluting).

The power density at any point in the core must be limited to maintain specified acceptable fuel design limits, including limits that preserve the criteria specified in 10 CFR 50.46 (Ref. 2). Together, LCO 3.1.6; LCO 3.2.4, "Departure from Nucleate Boiling Ratio (DNBR)," and LCO 3.2.5, "AXIAL SHAPE INDEX (ASI)," provide limits on control component operation and on monitored process variables to ensure the core operates within LCO 3.2.1, "Linear Heat Rate (LHR)," LCO 3.2.2, "Planar Radial Peaking Factor (Fxy)," and LCO 3.2.4, "Departure From Nucleate Boiling Ratio (DNBR)," limits in the COLR. Operation within the LHR limits given in the COLR prevents power peaks that would exceed

BASES

BACKGROUND (continued)

the loss of coolant accident (LOCA) limits derived by the Emergency Core Cooling Systems analysis. Operation within the F_{xy} and departure from nucleate boiling (DNB) limits given in the COLR prevents DNB during a loss of forced reactor coolant flow accident. In addition to the LHR, F_{xyxy}, and DNBR limits, certain reactivity limits are preserved by regulating CEA insertion limits. The regulating CEA insertion limits also restrict the ejected CEA worth to the values assumed in the safety analyses and preserve the minimum required SDM in MODES 1 and 2.

The establishment of limiting safety system settings and LCOs require that the expected long and short term behavior of the radial peaking factors be determined. The long term behavior relates to the variation of the steady state radial peaking factors with core burnup and is affected by the amount of CEA insertion assumed, the portion of a burnup cycle over which such insertion is assumed, and the expected power level variation throughout the cycle. The short term behavior relates to transient perturbations to the steady state radial peaks, due to radial xenon redistribution. The magnitudes of such perturbations depend upon the expected use of the CEAs during anticipated power reductions and load maneuvering. Analyses are performed, based on the expected mode of operation of the Nuclear Steam Supply System (base loaded, maneuvering, etc.). From these analyses, CEA insertions are determined and a consistent set of radial peaking factors defined. The long term steady state and short term insertion limits are determined, based upon the assumed mode of operation used in the analyses, and provide a means of preserving the assumptions on CEA insertions used. The long and short term insertion limits of LCO 3.1.6 are specified for the plant, which has been designed for primarily base loaded operation, but has the ability to accommodate a limited amount of load maneuvering.

The regulating CEA insertion and alignment limits, ASI and T_q, are process variables that together characterize and control the three dimensional power distribution of the reactor core. Additionally, the regulating bank insertion limits control the reactivity that could be added in the event of a CEA ejection accident, and the shutdown and regulating bank insertion limits ensure the required SDM is maintained.

Operation within the subject LCO limits will prevent fuel cladding failures that would breach the primary fission product barrier and release fission products to the reactor coolant in the event of a LOCA, loss of flow, ejected CEA, or other accident requiring termination by a Reactor Protection System trip function.

BASES

APPLICABLE SAFETY ANALYSES

The fuel cladding must not sustain damage as a result of normal operation (Condition I) and anticipated operational occurrences (Condition II). The acceptance criteria for the regulating CEA insertion, part length CEA insertion, ASI, and T_q LCOs preclude core power distributions from occurring that would violate the following fuel design criteria:

a. During a large break LOCA, the peak cladding temperature must not exceed a limit of 2200°F, 10 CFR 50.46 (Ref. 2),

b. During a loss of forced reactor coolant flow accident, there must be at least a 95% probability at a 95% confidence level (the 95/95 DNB criterion) that the hot fuel CEA in the core does not experience a DNB condition,

c. During an ejected CEA accident, the fission energy input to the fuel must not exceed 280 cal/gm (Ref. 3), and

d. The CEAs must be capable of shutting down the reactor with a minimum required SDM, with the highest worth CEA stuck fully withdrawn, GDC 26 (Ref. 1).

Regulating CEA position, ASI, and T_q are process variables that together characterize and control the three dimensional power distribution of the reactor core.

Fuel cladding damage does not occur when the core is operated outside these LCOs during normal operation. However, fuel cladding damage could result, should an accident occur with simultaneous violation of one or more of these LCOs. Changes in the power distribution can cause increased power peaking and corresponding increased local LHRs.

The SDM requirement is ensured by limiting the regulating and shutdown CEA insertion limits, so that the allowable inserted worth of the CEAs is such that sufficient reactivity is available in the CEAs to shut down the reactor to hot zero power with a reactivity margin that assumes the maximum worth CEA remains fully withdrawn upon trip (Ref. 4).

The most limiting SDM requirements for MODE 1 and 2 conditions at BOC are determined by the requirements of several transients, e.g., loss of flow, seized rotor, etc. However, the most limiting SDM requirements for MODES 1 and 2 at EOC come from just one transient, steam line break (SLB). The requirements of the SLB event at EOC for both the full power and no load conditions are significantly larger than those of any other event at that time in cycle and, also, considerably larger than the most limiting requirements at BOC.

BASES

APPLICABLE SAFETY ANALYSES (continued)

Although the most limiting SDM requirements at EOC are much larger than those at BOC, the available SDMs obtained via the scramming of the CEAs are also substantially larger due to the much lower boron concentration at EOC. To verify that adequate SDMs are available throughout the cycle to satisfy the changing requirements, calculations are performed at both BOC and EOC. It has been determined that calculations at these two times in cycle are sufficient since the differences between available SDMs and the limiting SDM requirements are the smallest at these times in cycle. The measurement of CEA bank worth performed as part of the Startup Testing Program demonstrates that the core has the expected shutdown capability. Consequently, adherance to LCOs 3.1.5 and 3.1.6 provides assurance that the available SDMs at any time in cycle will exceed the limiting SDM requirements at that time in cycle.

Operation at the insertion limits or ASI may approach the maximum allowable linear heat generation rate or peaking factor, with the allowed T_q present. Operation at the insertion limit may also indicate the maximum ejected CEA worth could be equal to the limiting value in fuel cycles that have sufficiently high ejected CEA worths.

The regulating and shutdown CEA insertion limits ensure that safety analyses assumptions for reactivity insertion rate, SDM, ejected CEA worth, and power distribution peaking factors are preserved (Ref. 5).

The regulating CEA insertion limits satisfy Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

The limits on regulating CEA sequence, overlap, and physical insertion, as defined in the COLR, must be maintained because they serve the function of preserving power distribution, ensuring that the SDM is maintained, ensuring that ejected CEA worth is maintained, and ensuring adequate negative reactivity insertion on trip. The overlap between regulating banks provides more uniform rates of reactivity insertion and withdrawal, and is imposed to maintain acceptable power peaking during regulating CEA motion.

The power dependent insertion limit (PDIL) alarm circuit is required to be OPERABLE for notification that the CEAs are outside the required insertion limits. When the PDIL alarm circuit is inoperable, the verification of CEA positions is increased to ensure improper CEA alignment is identified before unacceptable flux distribution occurs.

BASES

APPLICABILITY

The regulating CEA sequence, overlap, and physical insertion limits shall be maintained with the reactor in MODES 1 and 2. These limits must be maintained, since they preserve the assumed power distribution, ejected CEA worth, SDM, and reactivity rate insertion assumptions. Applicability in MODES 3, 4, and 5 is not required, since neither the power distribution nor ejected CEA worth assumptions would be exceeded in these MODES. SDM is preserved in MODES 3, 4, and 5 by adjustments to the soluble boron concentration.

This LCO is modified by a Note indicating the LCO requirement is suspended during SR 3.1.4.3. This SR verifies the freedom of the CEAs to move, and requires the regulating CEAs to move below the LCO limits, which would normally violate the LCO. The Note also allows the LCO to be not applicable during reactor power cutback operation, which inserts a selected CEA group (usually group 5) during loss of load events.

ACTIONS

A.1 and A.2

Operation beyond the transient insertion limit may result in a loss of SDM and excessive peaking factors. The transient insertion limit should not be violated during normal operation; this violation, however, may occur during transients when the operator is manually controlling the CEAs in response to changing plant conditions. When the regulating groups are inserted beyond the transient insertion limits, actions must be taken to either withdraw the regulating groups beyond the limits or to reduce THERMAL POWER to less than or equal to that allowed for the actual CEA insertion limit. Two hours provides a reasonable time to accomplish this, allowing the operator to deal with current plant conditions while limiting peaking factors to acceptable levels.

B.1 and B.2

If the CEAs are inserted between the long term steady state insertion limits, the transient insertion limits for intervals > 4 hours per 24 hour period, and the short term steady state insertion limits are exceeded, peaking factors can develop that are of immediate concern (Ref. 6).

Additionally, since the CEAs can be in this condition without misalignment, penalty factors are not inserted in the core protection calculators to compensate for the developing peaking factors. Verifying the short term steady state insertion limits are not exceeded ensures that the peaking factors that do develop are within those allowed for continued operation. Fifteen minutes provides adequate time for the operator to verify if the short term steady state insertion limits are exceeded.

BASES

ACTIONS (continued)

Experience has shown that rapid power increases in areas of the core, in which the flux has been depressed, can result in fuel damage as the LHR in those areas rapidly increases. Restricting the rate of THERMAL POWER increases to ≤ 5% RTP per hour, following CEA insertion beyond the long term steady state insertion limits, ensures the power transients experienced by the fuel will not result in fuel failure (Ref. 7).

C.1

With the regulating CEAs inserted between the long term steady state insertion limit and the transient insertion limit, and with the core approaching the 5 effective full power days (EFPD) per 30 EFPD, or 14 EFPD per 365 EFPD limits, the core approaches the acceptable limits placed on operation with flux patterns outside those assumed in the long term burnup assumptions. In this case, the CEAs must be returned to within the long term steady state insertion limits, or the core must be placed in a condition in which the abnormal fuel burnup cannot continue. A Completion Time of 2 hours is a reasonable time to return the CEAs to within the long term steady state insertion limits.

The required Completion Time of 2 hours from initial discovery of a regulating CEA group outside the limits until its restoration to within the long term steady state limits, shown on the figures in the COLR, allows sufficient time for borated water to enter the Reactor Coolant System from the chemical addition and makeup systems, and to cause the regulating CEAs to withdraw to the acceptable region. It is reasonable to continue operation for 2 hours after it is discovered that the 5 day or 14 day EFPD limit has been exceeded. This Completion Time is based on limiting the potential xenon redistribution, the low probability of an accident, and the steps required to complete the action.

D.1 and D.2

With the Core Operating Limit Supervisory System out of service, operation beyond the short term steady state insertion limits can result in peaking factors that could approach the DNB or local power density trip setpoints. Eliminating this condition within 2 hours limits the magnitude of the peaking factors to acceptable levels (Ref. 8). Restoring the CEAs to within the limit or reducing THERMAL POWER to that fraction of RTP that is allowed by CEA group position, using the limits specified in the COLR, ensures acceptable peaking factors are maintained.

BASES

ACTIONS (continued)

E.1

With the PDIL circuit inoperable, performing SR 3.1.6.1 within 1 hour and every 4 hours thereafter ensures improper CEA alignments are identified before unacceptable flux distributions occur.

F.1

When a Required Action cannot be completed within the required Completion Time, a controlled shutdown should be commenced. The allowed Completion Time of 6 hours is reasonable, based on operating experience, for reaching MODE 3 from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.1.6.1

With the PDIL alarm circuit OPERABLE, verification of each regulating CEA group position every 12 hours is sufficient to detect CEA positions that may approach the acceptable limits, and provides the operator with time to undertake the Required Action(s) should the sequence or insertion limits be found to be exceeded. The 12 hour Frequency also takes into account the indication provided by the PDIL alarm circuit and other information about CEA group positions available to the operator in the control room.

SR 3.1.6.1 is modified by a Note indicating that entry is allowed into MODE 2 for 12 hours without having performed the SR. This is necessary, since the unit must be in the applicable MODES in order to perform Surveillances that demonstrate the LCO limits are met.

SR 3.1.6.2

Verification of the accumulated time of CEA group insertion between the long term steady state insertion limits and the transient insertion limits ensures the cumulative time limits are not exceeded. The 24 hour Frequency ensures the operator identifies a time limit that is being approached before it is reached.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.1.6.3

Demonstrating the PDIL alarm circuit OPERABLE verifies that the PDIL alarm circuit is functional. The 31 day Frequency takes into account other Surveillances being performed at shorter Frequencies that identify improper CEA alignments.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 10 and GDC 26.
2. 10 CFR 50.46.
3. FSAR, Section [ ], Section [ ], and Section [ ].
4. FSAR, Section [ ].
5. FSAR, Section [ ].
6. FSAR, Section [ ].
7. FSAR, Section [ ].
8. FSAR, Section [ ].

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.7 Part Length Control Element Assembly (CEA) Insertion Limits (Digital)

BASES

BACKGROUND

The insertion limits of the part length control element assemblies (CEAs) are initial assumptions in all safety analyses. The insertion limits directly affect core power distributions. The applicable criteria for these power distribution design requirements are 10 CFR 50, Appendix A, GDC 10, "Reactor Design" (Ref. 1), and 10 CFR 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Nuclear Plants" (Ref. 2). Limits on part length CEA insertion have been established, and all CEA positions are monitored and controlled during power operation to ensure that the power distribution defined by the design power peaking limits is preserved.

The regulating CEAs are used for precise reactivity control of the reactor. The positions of the regulating CEAs are manually controlled. They are capable of adding reactivity very quickly (compared to borating or diluting).

The power density at any point in the core must be limited to maintain specified acceptable fuel design limits, including limits that preserve the criteria specified in 10 CFR 50.46 (Ref. 2). Together, LCO 3.1.6, "Regulating Control Element Assembly (CEA) Insertion Limits," LCO 3.1.7, LCO 3.2.4, "Departure From Nucleate Boiling Ratio (DNBR)," and LCO 3.2.5, "AXIAL SHAPE INDEX (ASI)," provide limits on control component operation and on monitored process variables to ensure the core operates within the linear heat rate (LHR) (LCO 3.2.1, "Linear Heat Rate (LHR)"), planar peaking factor (F_{xy}) (LCO 3.2.2, "Planar Radial Peaking Factors (F_{xy})"), and LCO 3.2.4 limits in the COLR.

Operation within the limits given in the COLR prevents power peaks that would exceed the loss of coolant accident (LOCA) limits derived by the Emergency Core Cooling Systems analysis. Operation within the F_{xy} and departure from nucleate boiling (DNB) limits given in the COLR prevents DNB during a loss of forced reactor coolant flow accident.

The establishment of limiting safety system settings and LCOs requires that the expected long and short term behavior of the radial peaking factors be determined. The long term behavior relates to the variation of the steady state radial peaking factors with core burnup; it is affected by the amount of CEA insertion assumed, the portion of a burnup cycle over which such insertion is assumed, and the expected power level variation throughout the cycle. The short term behavior relates to transient

BASES

BACKGROUND (continued)

perturbations to the steady state radial peaks due to radial xenon redistribution. The magnitudes of such perturbations depend upon the expected use of the CEAs during anticipated power reductions and load maneuvering. Analyses are performed, based on the expected mode of operation of the Nuclear Steam Supply System (base loaded, maneuvering, etc.). From these analyses, CEA insertions are determined, and a consistent set of radial peaking factors are defined. The long term (steady state) and short term insertion limits are determined, based upon the assumed mode of operation used in the analyses; they provide a means of preserving the assumptions on CEA insertions used. The long and short term insertion limits of LCO 3.1.7 are specified for the plant, which has been designed primarily for base loaded operation, but has the ability to accommodate a limited amount of load maneuvering.

APPLICABLE SAFETY ANALYSES

The fuel cladding must not sustain damage as a result of normal operation (Condition I) and anticipated operational occurrences (Condition II). The regulating CEA insertion, part length CEA insertion, ASI, and T_Q LCOs preclude core power distributions from occurring that would violate the following fuel design criteria:

a. During a large break LOCA, the peak cladding temperature must not exceed 2200°F (Ref. 2),

b. During a loss of forced reactor coolant flow accident, there must be at least a 95% probability at a 95% confidence level (the 95/95 DNB criterion) that the hot fuel CEA in the core does not experience a DNB condition,

c. During an ejected CEA accident, the fission energy input to the fuel must not exceed 280 cal/gm (Ref. 3), and

d. The CEAs must be capable of shutting down the reactor with a minimum required SDM, with the highest worth CEA stuck fully withdrawn, GDC 26 (Ref. 1).

Regulating CEA position, part length CEA position, ASI, and T_Q are process variables that together characterize and control the three dimensional power distribution of the reactor core.

BASES

APPLICABLE SAFETY ANALYSES (continued)

Fuel cladding damage does not occur when the core is operated outside these LCOs during normal operation. However, fuel cladding damage could result, should an accident occur with simultaneous violation of one or more of these LCOs. Changes in the power distribution can cause increased power peaking and corresponding increased local LHRs.

The regulating CEA insertion limits satisfy Criterion 2 of 10 CFR 50.36(c)(2)(ii). The part length CEAs are required due to the potential peaking factor violations that could occur if part length CEAs exceed insertion limits.

LCO

The limits on part length CEA insertion, as defined in the COLR, must be maintained because they serve the function of preserving power distribution.

APPLICABILITY

The part length insertion limits shall be maintained with the reactor in MODE 1 > 20% RTP. These limits must be maintained, since they preserve the assumed power distribution. Applicability in lower MODES is not required, since the power distribution assumptions would not be exceeded in these MODES.

This LCO has been modified by a Note suspending the LCO requirement while exercising part length CEAs. Exercising part length CEAs may require moving them outside their insertion limits.

ACTIONS

A.1, A.2, and B.1

If the part length CEA groups are inserted beyond the transient insertion limit or between the long term (steady state) insertion limit and the transient limit for 7 or more effective full power days (EFPD) out of any 30 EFPD period, or for 14 EFPD or more out of any 365 EFPD period, flux patterns begin to develop that are outside the range assumed for long term fuel burnup. If allowed to continue beyond this limit, the peaking factors assumed as initial conditions in the accident analysis may be invalidated (Ref. 4). Restoring the CEAs to within limits or reducing THERMAL POWER to that fraction of RTP that is allowed by CEA group position, using the limits specified in the COLR, ensures that acceptable peaking factors are maintained.

Since these effects are cumulative, actions are provided to limit the total time the part length CEAs can be out of limits in any 30 EFPD or 365 EFPD period. Since the cumulative out of limit times are in days, an additional Completion Time of 2 hours is reasonable for restoring the part length CEAs to within the allowed limits.

BASES

ACTIONS (continued)

C.1

When a Required Action cannot be completed within the required Completion Time, a controlled shutdown should commence. A Completion Time of 4 hours is reasonable, based on operating experience, for reducing power to ≤ 20 RTP from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.1.7.1

Verification of each part length CEA group position every 12 hours is sufficient to detect CEA positions that may approach the limits, and provide the operator with time to undertake the Required Action(s), should insertion limits be found to be exceeded. The 12 hour Frequency also takes into account the indication provided by the power dependent insertion limit alarm circuit and other information about CEA group positions available to the operator in the control room.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 10 and GDC 26.

2. 10 CFR 50.46.

3. FSAR, Section [ ].

4. FSAR, Section [ ].

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.8 Special Test Exceptions (STE) - SHUTDOWN MARGIN (SDM) (Digital)

BASES

BACKGROUND

The primary purpose of the SHUTDOWN MARGIN (SDM) Special Test Exceptions (STE) is to permit relaxation of existing LCOs to allow the performance of certain PHYSICS TESTS. These tests are conducted to determine the control element assembly (CEA) worth.

Section XI of 10 CFR 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Processing Plants" (Ref. 1), requires that a test program be established to ensure that structures, systems, and components will perform satisfactorily in service. All functions necessary to ensure that specified design conditions are not exceeded during normal operation and anticipated operational occurrences must be tested. Testing is required as an integral part of the design, fabrication, construction, and operation of the power plant. Requirements for notification of the NRC, for the purpose of conducting tests and experiments, are specified in 10 CFR 50.59, "Changes, Tests, and Experiments" (Ref. 2).

The key objectives of a test program are to (Ref. 3):

a. Ensure that the facility has been adequately designed,

b. Validate the analytical models used in design and analysis,

c. Verify assumptions used for predicting plant response,

d. Ensure that installation of equipment in the facility has been accomplished in accordance with the design, and

e. Verify that operating and emergency procedures are adequate.

To accomplish these objectives, testing is required prior to initial criticality, after each refueling shutdown, and during startup, low power operation, power ascension, and at power operation. The PHYSICS TESTS requirements for reload fuel cycles ensure that the operating characteristics of the core are consistent with the design predictions and that the core can be operated as designed (Ref. 4).

BASES

BACKGROUND (continued)

PHYSICS TESTS procedures are written and approved in accordance with established formats. The procedures include all information necessary to permit a detailed execution of testing required to ensure that the design intent is met. PHYSICS TESTS are performed in accordance with these procedures and test results are approved prior to continued power escalation and long term power operation. Examples of PHYSICS TESTS include determination of critical boron concentration, CEA group worths, reactivity coefficients, flux symmetry, and core power distribution.

APPLICABLE SAFETY ANALYSES

It is acceptable to suspend certain LCOs for PHYSICS TESTS because fuel damage criteria are not exceeded. Even if an accident occurs during PHYSICS TESTS with one or more LCOs suspended, fuel damage criteria are preserved because adequate limits on power distribution and shutdown capability are maintained during PHYSICS TESTS.

Reference 5 defines the requirements for initial testing of the facility, including PHYSICS TESTS. Requirements for reload fuel cycle PHYSICS TESTS are defined in ANSI/ANS-19.6.1-1985 (Ref. 4). PHYSICS TESTS for reload fuel cycles are given in Table 1 of ANSI/ANS-19.6.1-1985. Although these PHYSICS TESTS are generally accomplished within the limits of all LCOs, conditions may occur when one or more LCOs must be suspended to make completion of PHYSICS TESTS possible or practical. This is acceptable as long as the fuel design criteria are not violated. As long as the linear heat rate (LHR) remains within its limit, fuel design criteria are preserved.

In this test, the following LCOs are suspended:

a. LCO 3.1.1, "SHUTDOWN MARGIN (SDM),"

b. LCO 3.1.5, “Shutdown Control Element Assembly (CEA) Insertion Limits,” and

c. LCO 3.1.6, "Regulating Control Element Assembly (CEA) Insertion Limits."

Therefore, this LCO places limits on the minimum amount of CEA worth required to be available for reactivity control when CEA worth measurements are performed.

The individual LCOs cited above govern SDM CEA group height, insertion, and alignment. Additionally, the LCOs governing Reactor Coolant System (RCS) flow, reactor inlet temperature T_c, and pressurizer pressure contribute to maintaining departure from nucleate boiling (DNB) parameter limits. The initial condition criteria for accidents sensitive to

BASES

APPLICABLE SAFETY ANALYSES (continued)

core power distribution are preserved by the LHR and DNB parameter limits. The criteria for the loss of coolant accident (LOCA) are specified in 10 CFR 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Nuclear Power Reactors" (Ref. 6). The criteria for the loss of forced reactor coolant flow accidents are specified in Reference 7. Operation within the LHR limit preserves the LOCA criteria; operation within the DNB parameter limits preserves the loss of flow criteria.

SRs are conducted as necessary to ensure that LHR and DNB parameters remain within limits during PHYSICS TESTS. Performance of these SRs allows PHYSICS TESTS to be conducted without decreasing the margin of safety.

Requiring that shutdown reactivity equivalent to at least the highest estimated CEA worth (of those CEAs actually withdrawn) be available for trip insertion from the OPERABLE CEAs, provides a high degree of assurance that shutdown capability is maintained for the most challenging postulated accident, a stuck CEA. Since LCO 3.1.1 is suspended, however, there is not the same degree of assurance during this test that the reactor would always be shut down if the highest worth CEA was stuck out and calculational uncertainties or the estimated highest CEA worth was not as expected (the single failure criterion is not met). This situation is judged acceptable, however, because specified acceptable fuel damage limits are still met. The risk of experiencing a stuck CEA and subsequent criticality is reduced during this PHYSICS TEST exception by the requirements to determine CEA positions every 2 hours; by the trip of each CEA to be withdrawn within 24 hours prior to suspending the SDM; and by ensuring that shutdown reactivity is available, equivalent to the reactivity worth of the estimated highest worth withdrawn CEA (Ref. 5).

PHYSICS TESTS include measurement of core parameters or exercise of control components that affect process variables. Among the process variables involved are total planar radial peaking factor, total integrated radial peaking factor, T_Q, and ASI, which represent initial condition input (power peaking) to the accident analysis. Also involved are the shutdown and regulating CEAs, which affect power peaking and are required for shutdown of the reactor. The limits for these variables are specified for each fuel cycle in the COLR.

As described in LCO 3.0.7, compliance with Special Test Exception LCOs is optional, and therefore no criteria of 10 CFR 50.36(c)(2)(ii) apply. Special Test Exception LCOs provide flexibility to perform certain operations by appropriately modifying requirements of other LCOs. A discussion of the criteria satisfied for the other LCOs is provided in their respective Bases.

BASES

LCO

This LCO provides that a minimum amount of CEA worth is immediately available for reactivity control when CEA worth measurement tests are performed. This STE is required to permit the periodic verification of the actual versus predicted worth of the regulating and shutdown CEAs. The SDM requirements of LCO 3.1.1, the shutdown CEA insertion limits of LCO 3.1.5, and the regulating CEA insertion limits of LCO 3.1.6 may be suspended.

APPLICABILITY

This LCO is applicable in MODES 2 and 3. Although CEA worth testing is conducted in MODE 2, sufficient negative reactivity is inserted during the performance of these tests to result in temporary entry into MODE 3. Because the intent is to immediately return to MODE 2 to continue CEA worth measurements, the STE allows limited operation to 6 consecutive hours in MODE 3 as indicated by the Note, without having to borate to meet the SDM requirements of LCO 3.1.1.

ACTIONS

A.1

With any CEA not fully inserted and less than the minimum required reactivity equivalent available for insertion, or with all CEAs inserted and the reactor subcritical by less than the reactivity equivalent of the highest worth withdrawn CEA, restoration of the minimum SDM requirements must be accomplished by increasing the RCS boron concentration. The required Completion Time of 15 minutes for initiating boration allows the operator sufficient time to align the valves and start the boric acid pumps and is consistent with the Completion Time of LCO 3.1.1.

SURVEILLANCE REQUIREMENTS

SR 3.1.8.1

Verification of the position of each partially or fully withdrawn full length or part length CEA is necessary to ensure that the minimum negative reactivity requirements for insertion on a trip are preserved. A 2 hour Frequency is sufficient for the operator to verify that each CEA position is within the acceptance criteria.

SR 3.1.8.2

Prior demonstration that each CEA to be withdrawn from the core during PHYSICS TESTS is capable of full insertion, when tripped from at least a 50% withdrawn position, ensures that the CEA will insert on a trip signal. The Frequency ensures that the CEAs are OPERABLE prior to reducing SDM to less than the limits of LCO 3.1.1.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The SR is modified by a Note which allows the SR to not be performed during initial power escalation following a refueling outage if SR 3.1.4.5 has been met during that refueling outage. This allows the CEA drop time test, which also proves the CEAs are trippable, to be credited for this SR.

REFERENCES

1. 10 CFR 50, Appendix B, Section XI.
2. 10 CFR 50.59.
3. Regulatory Guide 1.68, Revision 2, August 1978.
4. ANSI/ANS-19.6.1-1985, December 13, 1985.
5. FSAR, Chapter 14.
6. 10 CFR 50.46.
7. FSAR, Chapter 15.

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.9 Special Test Exceptions (STE) - MODES 1 and 2 (Digital)

BASES

BACKGROUND

The primary purpose of these MODES 1 and 2 Special Test Exceptions (STE) is to permit relaxation of existing LCOs to allow the performance of certain PHYSICS TESTS. These tests are conducted to determine specific reactor core characteristics.

Section XI of 10 CFR 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Processing Plants" (Ref. 1), requires that a test program be established to ensure that structures, systems, and components will perform satisfactorily in service. All functions necessary to ensure that specified design conditions are not exceeded during normal operation and anticipated operational occurrences must be tested. Testing is required as an integral part of the design, fabrication, construction, and operation of the power plant. Requirements for notification of the NRC, for the purpose of conducting tests and experiments, are specified in 10 CFR 50.59, "Changes, Tests, and Experiments" (Ref. 2).

The key objectives of a test program are to (Ref. 3):

a. Ensure that the facility has been adequately designed,

b. Validate the analytical models used in design and analysis,

c. Verify assumptions used for predicting plant response,

d. Ensure that installation of equipment in the facility has been accomplished in accordance with design, and

e. Verify that operating and emergency procedures are adequate.

To accomplish these objectives, testing is required prior to initial criticality, after each refueling shutdown, and during startup, low power operation, power ascension, and at power operation. The PHYSICS TESTS requirements for reload fuel cycles ensure that the operating characteristics of the core are consistent with the design predictions and that the core can be operated as designed (Ref. 4).

PHYSICS TESTS procedures are written and approved in accordance with established formats. The procedures include all information necessary to permit a detailed execution of testing required to ensure that design intent is met. PHYSICS TESTS are performed in accordance with these procedures and test results are approved prior to continued power escalation and long term power operation.

BASES

BACKGROUND (continued)

Examples of PHYSICS TESTS include determination of critical boron concentration, CEA group worths, reactivity coefficients, flux symmetry, and core power distribution.

APPLICABLE SAFETY ANALYSES

It is acceptable to suspend certain LCOs for PHYSICS TESTS because fuel damage criteria are not exceeded. Even if an accident occurs during PHYSICS TESTS with one or more LCOs suspended, fuel damage criteria are preserved because the limits on power distribution and shutdown capability are maintained during PHYSICS TESTS.

Reference 5 defines requirements for initial testing of the facility, including PHYSICS TESTS. Requirements for reload fuel cycle PHYSICS TESTS are defined in ANSI/ANS-19.6.1-1985 (Ref. 4). Although these PHYSICS TESTS are generally accomplished within the limits of all LCOs, conditions may occur when one or more LCOs must be suspended to make completion of PHYSICS TESTS possible or practical. This is acceptable as long as the fuel design criteria are not violated. As long as the linear heat rate (LHR) remains within its limit, fuel design criteria are preserved.

In this test, the following LCOs are suspended:

LCO 3.1.3, "Moderator Temperature Coefficient (MTC),"
LCO 3.1.4, "Control Element Assembly (CEA) Alignment,"
LCO 3.1.5, "Shutdown Control Element Assembly (CEA) Insertion Limits,"
LCO 3.1.6, "Regulating Control Element Assembly (CEA) Insertion Limits,"
LCO 3.1.7, "Part Length Control Element Assembly (CEA) Insertion Limits,"
LCO 3.2.2, "Planar Radial Peaking Factors," and
LCO 3.2.3, "AZIMUTHAL POWER TILT (T_q)."

The safety analysis (Ref. 6) places limits on allowable THERMAL POWER during PHYSICS TESTS and requires that the LHR and the departure from nucleate boiling (DNB) parameter be maintained within limits. The power plateau of < 85% RTP and the associated trip setpoints are required to ensure [explain].

The individual LCOs governing CEA group height, insertion and alignment, ASI, total planar radial peaking factor, total integrated radial peaking factor, and T_q, preserve the LHR limits. Additionally, the LCOs governing Reactor Coolant System (RCS) flow, reactor inlet temperature (T_c), and pressurizer pressure contribute to maintaining DNB parameter

BASES

APPLICABLE SAFETY ANALYSES (continued)

limits. The initial condition criteria for accidents sensitive to core power distribution are preserved by the LHR and DNB parameter limits. The criteria for the loss of coolant accident (LOCA) are specified in 10 CFR 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Nuclear Power Reactors" (Ref. 7). The criteria for the loss of forced reactor coolant flow accident are specified in Reference 7. Operation within the LHR limit preserves the LOCA criteria; operation within the DNB parameter limits preserves the loss of flow criteria.

During PHYSICS TESTS, one or more of the LCOs that normally preserve the LHR and DNB parameter limits may be suspended. The results of the accident analysis are not adversely impacted, however, if LHR and DNB parameters are verified to be within their limits while the LCOs are suspended. Therefore, SRs are placed as necessary to ensure that LHR and DNB parameters remain within limits during PHYSICS TESTS. Performance of these Surveillances allows PHYSICS TESTS to be conducted without decreasing the margin of safety.

PHYSICS TESTS include measurement of core parameters or exercise of control components that affect process variables. Among the process variables involved are total planar radial peaking factor, total integrated radial peaking factor, T_Q, and ASI, which represent initial condition input (power peaking) to the accident analysis. Also involved are the shutdown and regulating CEAs, which affect power peaking and are required for shutdown of the reactor. The limits for these variables are specified for each fuel cycle in the COLR.

As described in LCO 3.0.7, compliance with Special Test Exception LCOs is optional, and therefore no criteria of 10 CFR 50.36(c)(2)(ii) apply. Special Test Exception LCOs provide flexibility to perform certain operations by appropriately modifying requirements of other LCOs. A discussion of the criteria satisfied for the other LCOs is provided in their respective Bases.

LCO

This LCO permits individual CEAs to be positioned outside of their normal group heights and insertion limits during the performance of PHYSICS TESTS, such as those required to:

a. Measure CEA worth,

b. Determine the reactor stability index and damping factor under xenon oscillation conditions,

c. Determine power distributions for nonnormal CEA configurations,

BASES

LCO (continued)

d. Measure rod shadowing factors, and

e. Measure temperature and power coefficients.

Additionally, it permits the center CEA to be misaligned during PHYSICS TESTS required to determine the isothermal temperature coefficient (ITC), MTC, and power coefficient.

The requirements of LCO 3.1.3, LCO 3.1.4, LCO 3.1.5, LCO 3.1.6, LCO 3.1.7, LCO 3.2.2, and LCO 3.2.3 may be suspended during the performance of PHYSICS TESTS provided THERMAL POWER is restricted to test power plateau, which shall not exceed 85% RTP.

APPLICABILITY

This LCO is applicable in MODES 1 and 2 because the reactor must be critical at various THERMAL POWER levels to perform the PHYSICS TESTS described in the LCO section. Limiting the test power plateau to < 85% RTP ensures that LHRs are maintained within acceptable limits.

ACTIONS

A.1

If THERMAL POWER exceeds the test power plateau in MODE 1, THERMAL POWER must be reduced to restore the additional thermal margin provided by the reduction. The 15 minute Completion Time ensures that prompt action shall be taken to reduce THERMAL POWER to within acceptable limits.

B.1 and B.2

If Required Action A.1 cannot be completed within the required Completion Time, PHYSICS TESTS must be suspended within 1 hour. Allowing 1 hour for suspending PHYSICS TESTS allows the operator sufficient time to change any abnormal CEA configuration back to within the limits of LCO 3.1.4, LCO 3.1.5, and LCO 3.1.6.

Suspension of PHYSICS TESTS exceptions requires restoration of each of the applicable LCOs to within specification.

BASES

SURVEILLANCE REQUIREMENTS	SR 3.1.9.1 Verifying that THERMAL POWER is equal to or less than that allowed by the test power plateau, as specified in the PHYSICS TEST procedure and required by the safety analysis, ensures that adequate LHR and departure from nucleate boiling ratio margins are maintained while LCOs are suspended. The 1 hour Frequency is sufficient, based upon the slow rate of power change and increased operational controls in place during PHYSICS TESTS. Monitoring LHR ensures that the limits are not exceeded.
REFERENCES	1. 10 CFR 50, Appendix B, Section XI. 2. 10 CFR 50.59. 3. Regulatory Guide 1.68, Revision 2, August 1978. 4. ANSI/ANS-19.6.1-1985, December 13, 1985. 5. FSAR, Chapter [14]. 6. FSAR, Section [15.3.2.1]. 7. 10 CFR 50.46.

B 3.2 POWER DISTRIBUTION LIMITS

B 3.2.1 Linear Heat Rate (LHR) (Analog)

BASES

BACKGROUND

The purpose of this LCO is to limit the core power distribution to the initial values assumed in the accident analyses. Operation within the limits imposed by this LCO either limits or prevents potential fuel cladding failures that could breach the primary fission product barrier and release fission products to the reactor coolant in the event of a loss of coolant accident (LOCA), loss of flow accident, ejected control element assembly (CEA) accident, or other postulated accident requiring termination by a Reactor Protection System trip function. This LCO limits the amount of damage to the fuel cladding during an accident by ensuring that the plant is operating within acceptable bounding conditions at the onset of a transient.

Methods of controlling the power distribution include:

a. Using CEAs to alter the axial power distribution,

b. Decreasing CEA insertion by boration, thereby improving the radial power distribution, and

c. Correcting off optimum conditions (e.g., a CEA drop or misoperation of the unit) that cause margin degradations.

The core power distribution is controlled so that, in conjunction with other core operating parameters (e.g., CEA insertion and alignment limits), the power distribution satisfies this LCO. The limiting safety system settings and this LCO are based on the accident analyses (Refs. 1 and 2), so that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences (AOOs), and the limits of acceptable consequences are not exceeded for other postulated accidents.

Limiting power distribution skewing over time also minimizes the xenon distribution skewing, which is a significant factor in controlling the axial power distribution.

Power distribution is a product of multiple parameters, various combinations of which may produce acceptable power distributions. Operation within the design limits of power distribution is accomplished by generating operating limits on linear heat rate (LHR) and departure from nucleate boiling (DNB).

BASES

BACKGROUND (continued)

The limits on LHR, Total Planar Radial Peaking Factor (F^T_{XY}), Total Integrated Radial Peaking Factor ($F^T{}_r$), T_q, and ASI represent limits within which the LHR algorithms are valid. These limits are obtained directly from the core reload analysis.

Either of the two core power distribution monitoring systems, the Excore Detector Monitoring System or the Incore Detector Monitoring System, provides adequate monitoring of the core power distribution and is capable of verifying that the LHR is within its limits. The Excore Detector Monitoring System performs this function by continuously monitoring ASI with the OPERABLE quadrant symmetric excore neutron flux detectors and verifying that the ASI is maintained within the allowable limits specified in the COLR.

In conjunction with the use of the Excore Detector Monitoring System and in establishing ASI limits, the following assumptions are made:

a. The CEA insertion limits of LCO 3.1.5, "Shutdown CEA Insertion Limits," and LCO 3.1.6, "Regulating CEA Insertion Limits," are satisfied,

b. The T_q restrictions of LCO 3.2.4 are satisfied, and

c. F^T_{xy} is within the limits of LCO 3.2.2.

The Incore Detector Monitoring System continuously provides a more direct measure of the peaking factors and alarms that have been established for the individual incore detector segments, ensuring that the peak LHRs are maintained within the limits specified in the COLR. The setpoints for these alarms include tolerances, set in conservative directions, for:

a. A measurement calculational uncertainty factor of 1.062,

b. An engineering uncertainty factor of 1.03,

c. An allowance of 1.002 for axial fuel densification and thermal expansion, and

d. A THERMAL POWER measurement uncertainty factor of 1.02.

BASES

APPLICABLE SAFETY ANALYSES

The fuel cladding must not sustain damage as a result of normal operation (Condition 1) and AOOs (Condition 2) (Ref. 3, GDC 10). The power distribution and CEA insertion and alignment LCOs preclude core power distributions that violate the following fuel design criteria:

a. During a LOCA, peak cladding temperature must not exceed 2200°F (Ref. 4),

b. During a loss of flow accident, there must be at least 95% probability at the 95% confidence level (the 95/95 DNB criterion) that the hot fuel rod in the core does not experience a DNB condition (Ref. 3, GDC 10),

c. During an ejected CEA accident, the fission energy input to the fuel must not exceed 280 cal/gm (Ref. [ ]), and

d. The control rods must be capable of shutting down the reactor with a minimum required SDM with the highest worth control rod stuck fully withdrawn (Ref. 3, GDC 26).

The power density at any point in the core must be limited to maintain the fuel design criteria (Ref. 4). This is accomplished by maintaining the power distribution and reactor coolant conditions so that the peak LHR and DNB parameters are within operating limits supported by accident analyses (Ref. 1), with due regard for the correlations between measured quantities, the power distribution, and uncertainties in determining the power distribution.

Fuel cladding failure during a LOCA is limited by restricting the maximum linear heat generation rate so that the peak cladding temperature does not exceed 2200°F (Ref. 4). High peak cladding temperatures are assumed to cause severe cladding failure by oxidation due to a Zircaloy water reaction.

The LCOs governing LHR, ASI, and the Reactor Coolant System ensure that these criteria are met as long as the core is operated within the ASI, F_{XY}^T, F_r^T, and T_q limits specified in the COLR. The latter are process variables that characterize the three dimensional power distribution of the reactor core. Operation within the limits for these variables ensures that their actual values are within the ranges used in the accident analyses.

BASES

APPLICABLE SAFETY ANALYSES (continued)

Fuel cladding damage does not normally occur while the unit is operating at conditions outside the limits of these LCOs during normal operation. Fuel cladding damage could result, however, if an accident or AOO occurs from initial conditions outside the limits of these LCOs. The potential for fuel cladding damage exists because changes in the power distribution can cause increased power peaking and can correspondingly increase local LHR.

The LHR satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

The power distribution LCO limits are based on correlations between power peaking and certain measured variables used as inputs to the LHR and DNB ratio operating limits. The power distribution LCO limits, except T_q, are provided in the COLR. The limitation on the LHR ensures that, in the event of a LOCA, the peak temperature of the fuel cladding does not exceed 2200°F.

APPLICABILITY

In MODE 1, power distribution must be maintained within the limits assumed in the accident analysis to ensure that fuel damage does not result following an AOO. In other MODES, this LCO does not apply because there is not sufficient THERMAL POWER to require a limit on the core power distribution.

ACTIONS

A.1

With the LHR exceeding its limit, excessive fuel damage could occur following an accident. In this Condition, prompt action must be taken to restore the LHR to within the specified limits. One hour to restore the LHR to within its specified limits is reasonable and ensures that the core does not continue to operate in this Condition. The 1 hour Completion Time also allows the operator sufficient time for evaluating core conditions and for initiating proper corrective actions.

B.1

If the LHR cannot be returned to within its specified limits, THERMAL POWER must be reduced. The change to MODE 2 provides reasonable assurance that the core is operating within its thermal limits and places the core in a conservative condition. The allowed Completion Time of 6 hours is reasonable, based on operating experience, to reach MODE 2 from full power MODE 1 conditions in an orderly manner and without challenging plant systems.

BASES

SURVEILLANCE REQUIREMENTS

A Note was added to the SRs to require LHR to be determined by either the Excore Detector Monitoring System or the Incore Detector Monitoring System.

SR 3.2.1.1

Performance of this SR verifies that the Excore Detector Monitoring System can accurately monitor the LHR. Therefore, this SR is only applicable when the Excore Detector Monitoring System is being used to determine the LHR. The 31 day Frequency is appropriate for this SR because it is consistent with the requirements of SR 3.3.1.3 for calibration of the excore detectors using the incore detectors.

The SR is modified by a Note that states that the SR is only required to be met when the Excore Detection Monitoring System is being used to determine LHR. The reason for the Note is that the excore detectors input neutron flux information into the ASI calculation.

SR 3.2.1.2 and SR 3.2.1.3

Continuous monitoring of the LHR is provided by the Incore Detector Monitoring System and the Excore Detector Monitoring System. Either of these two core power distribution monitoring systems provides adequate monitoring of the core power distribution and is capable of verifying that the LHR does not exceed its specified limits.

Performance of these SRs verifies that the Incore Detector Monitoring System can accurately monitor LHR. Therefore, they are only applicable when the Incore Detector Monitoring System is being used to determine the LHR.

A 31 day Frequency is consistent with the historical testing frequency of the reactor monitoring system. The SRs are modified by two Notes. Note 1 allows the SRs to be met only when the Incore Detector Monitoring System is being used to determine LHR. Note 2 states that the SRs are not required to be performed when THERMAL POWER is < 20% RTP. The accuracy of the neutron flux information from the incore detectors is not reliable at THERMAL POWER < 20% RTP.

BASES

REFERENCES	1.	FSAR, Chapter [15].
	2.	FSAR, Chapter [6].
	3.	10 CFR 50, Appendix A.
	4.	10 CFR 50.46.

B 3.2 POWER DISTRIBUTION LIMITS

B 3.2.2 Total Planar Radial Peaking Factor (F^T_{XY}) (Analog)

BASES

BACKGROUND

The purpose of this LCO (Total Planar Radial Peaking Factor (F^T_{XY})) is to limit the core power distribution to the initial values assumed in the accident analyses. Operation within the limits imposed by this LCO decreases or prevents potential fuel cladding failures that could breach the primary fission product barrier and release fission products to the reactor coolant in the event of a loss of coolant accident (LOCA), loss of flow accident, ejected control element assembly (CEA) accident, or other postulated accident requiring termination by a Reactor Protection System trip function. This LCO limits damage to the fuel cladding during an accident by ensuring that the plant is operating within acceptable bounding conditions at the onset of a transient.

Methods of controlling the power distribution include:

a. Using CEAs to alter the axial power distribution,

b. Decreasing CEA insertion by boration, thereby improving the radial power distribution, and

c. Correcting off optimum conditions (e.g., a CEA drop or misoperation of the unit) that cause margin degradations.

The core power distribution is controlled so that, in conjunction with other core operating parameters (e.g., CEA insertion and alignment limits), the power distribution does not result in violation of this LCO. The limiting safety system settings (LSSS) and this LCO are based on accident analyses (Refs. 1 and 2), so that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences (AOOs) and the limits of acceptable consequences are not exceeded for other postulated accidents.

Limiting power distribution skewing over time also minimizes the xenon distribution skewing, which is a significant factor in controlling the axial power distribution.

Power distribution is a product of multiple parameters, various combinations of which may produce acceptable power distributions. Operation within the design limits of power distribution is accomplished by generating operating limits on the linear heat rate (LHR) and departure from nucleate boiling (DNB).

BASES

BACKGROUND (continued)

The limits on LHR, F^T_{XY}, Total Integrated Radial Peaking Factor (F^T_r), T_q, and ASI represent limits within which the LHR algorithms are valid. These limits are obtained directly from the core reload analysis.

Either of the two core power distribution monitoring systems, the Excore Detector Monitoring System or the Incore Detector Monitoring System, provides adequate monitoring of the core power distribution and is capable of verifying that the LHR does not exceed its limits. The Excore Detector Monitoring System performs this function by continuously monitoring the ASI with the OPERABLE quadrant symmetric excore neutron flux detectors and verifying that the ASI is maintained within the allowable limits specified in the COLR.

In conjunction with the use of the Excore Detector Monitoring System and in establishing the ASI limits, the following assumptions are made:

a. The CEA insertion limits of LCO 3.1.5, "Shutdown CEA Insertion Limits," and LCO 3.1.6, "Regulating CEA Insertion Limits," are satisfied,

b. The T_q restrictions of LCO 3.2.4 are satisfied, and

c. F^T_{XY} does not exceed the limits of this LCO.

The Incore Detector Monitoring System continuously provides a more direct measure of the peaking factors, and the alarms that have been established for the individual incore detector segments ensure that the peak LHRs are maintained within the limits specified in the COLR. The setpoints for these alarms include tolerances, set in conservative directions, for:

a. A measurement calculational uncertainty factor of 1.062,

b. An engineering uncertainty factor of 1.03,

c. An allowance of 1.002 for axial fuel densification and thermal expansion, and

d. A THERMAL POWER measurement uncertainty factor of 1.02.

BASES

APPLICABLE SAFETY ANALYSES

The fuel cladding must not sustain damage as a result of normal operation (Condition 1) or AOOs (Condition 2) (Ref. 3, GDC 10). The Power Distribution and CEA Insertion and Alignment LCOs preclude core power distributions that violate the following fuel design criteria:

a. During a LOCA, peak cladding temperature must not exceed 2200°F (Ref. 4),

b. During a loss of flow accident, there must be at least 95% probability at the 95% confidence level (the 95/95 DNB criterion) that the hot fuel rod in the core does not experience a DNB condition (Ref. 3, GDC 10),

c. During an ejected CEA accident, the fission energy input to the fuel must not exceed 280 cal/gm (Ref. [ ]), and

d. The control rods must be capable of shutting down the reactor with a minimum required SDM with the highest worth control rod stuck, fully withdrawn (Ref. 3, GDC 26).

The power density at any point in the core must be limited to maintain the fuel design criteria (Ref. 4). This limiting is accomplished by maintaining the power distribution and reactor coolant conditions such that the peak LHR and DNB parameters are within operating limits supported by the accident analyses (Ref. 1) with due regard for the correlations between measured quantities, the power distribution, and the uncertainties in the determination of power distribution.

Fuel cladding failure during a LOCA is limited by restricting the maximum linear heat generation rate so that the peak cladding temperature does not exceed 2200°F (Ref. 4). High peak cladding temperatures are assumed to cause severe cladding failure by oxidation due to a Zircaloy water reaction.

The LCOs governing LHR, ASI, and the Reactor Coolant System ensure that these criteria are met as long as the core is operated within the ASI, F_{XY}^{T}, F_{r}^{T}, and T_q limits specified in the COLR. The latter are process variables that characterize the three dimensional power distribution of the reactor core. Operation within the limits for these variables ensures that their actual values are within the ranges used in the accident analyses.

BASES

APPLICABLE SAFETY ANALYSES (continued)

Fuel cladding damage does not normally occur while at conditions outside the limits of these LCOs during normal operation. Fuel cladding damage could result, however, should an accident or AOO occur from initial conditions outside the limits of these LCOs. This potential for fuel cladding damage exists because changes in the power distribution can cause increased power peaking and correspondingly increased local LHR.

F^T_{XY} satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

The power distribution LCO limits are based on correlations between power peaking and certain measured variables used as inputs to the LHR and DNB ratio operating limits. The power distribution LCO limits, except T_q, are provided in the COLR. The limitation on LHR ensures that in the event of a LOCA the peak temperature of the fuel cladding does not exceed 2200°F.

APPLICABILITY

In MODE 1, power distribution must be maintained within the limits assumed in the accident analyses to ensure that fuel damage does not result following an AOO. In other MODES, this LCO does not apply because there is not sufficient THERMAL POWER to require a limit on the core power distribution.

ACTIONS

A.1 and A.2

A Note modifies Condition A to require Required Actions A.1 and A.2 to be completed if the Condition is entered. This ensures that corrective action is taken prior to unrestricted operation.

The limitations on F^T_{XY} provided in the COLR ensure that the assumptions used in the analysis for establishing the LHR, LCO, and LSSS remain valid during operation at the various allowable CEA group insertion limits. If F^T_{XY} exceeds its basic limitation, operation may continue under the additional restrictions imposed by these Required Actions (reducing THERMAL POWER and withdrawing CEAs to or beyond the long term steady state insertion limits of LCO 3.1.6), because these additional restrictions adequately ensure that the assumptions used in establishing the LHR, LCO, and LSSS remain valid (Ref. 3). Six hours to return F^T_{XY} to within its limit is reasonable and ensures that all CEAs meet the long term steady state insertion limits of LCO 3.1.6.

BASES

ACTIONS (continued)

B.1

If F^T_r cannot be returned to within its limit, THERMAL POWER must be reduced. A change to MODE 2 provides reasonable assurance that the core is operating within its thermal limits and places the core in a conservative condition. The allowed Completion Time of 6 hours is reasonable, based on operating experience, to reach MODE 2 from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.2.2.1

The periodic Surveillance to determine the calculated F^T_{XY} ensures that F^T_{XY} remains within the range assumed in the analysis throughout the fuel cycle. Determining the measured F^T_{XY} after each fuel loading prior to the reactor exceeding 70% RTP ensures that the core is properly loaded.

Performance of the Surveillance every 31 days of accumulated operation in MODE 1 provides reasonable assurance that unacceptable changes in the F^T_{XY} are promptly detected.

The power distribution map can only be obtained after THERMAL POWER exceeds 20% RTP because the incore detectors are not reliable below 20% RTP.

The SR is modified by a Note that requires that SR 3.2.2.2 and SR 3.2.2.3 be completed each time SR 3.2.1.1 is completed. (Values computed by these SRs are required to perform SR 3.2.2.1.) The Note also requires that the incore detectors be used to determine F^T_{XY} by using them to obtain a power distribution map with all full length CEAs above the long term steady state insertion limits, as specified in the COLR.

SR 3.2.2.2 and SR 3.2.2.3

Measuring the value of F_{XY} and T_q each time a calculated value of F^T_{XY} is required ensures that the calculated value of F^T_{XY} accurately reflects the condition of the core.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The Frequency for these Surveillances is in accordance with the Frequency requirements of SR 3.2.2.1, because these SRs provide information to complete SR 3.2.2.1.

REFERENCES

1. FSAR, Chapter [15].
2. FSAR, Chapter [6].
3. 10 CFR 50, Appendix A.
4. 10 CFR 50.46.

B 3.2 POWER DISTRIBUTION LIMITS

B 3.2.3 Total Integrated Radial Peaking Factor (F^T_{XY}) (Analog)

BASES

BACKGROUND

The purpose of this LCO (Total Integrated Radial Peaking Factor ($F^T{}_r$)) is to limit the core power distribution to the initial values assumed in the accident analyses. Operation within the limits imposed by this LCO either limits or prevents potential fuel cladding failures that could breach the primary fission product barrier and release fission products to the reactor coolant in the event of a loss of coolant accident (LOCA), loss of flow accident, ejected control element assembly (CEA) accident, or other postulated accident requiring termination by a Reactor Protection System trip function. This LCO limits the amount of damage to the fuel cladding during an accident by ensuring that the plant is operating within acceptable bounding conditions at the onset of a transient.

Methods of controlling the power distribution include:

a. The use of CEAs to alter the axial power distribution,

b. Decreasing CEA insertion by boration, thereby improving the radial power distribution, and

c. Correcting off optimum conditions (e.g., a CEA drop or misoperation of the unit) that cause margin degradations.

The core power distribution is controlled so that, in conjunction with other core operating parameters (e.g., CEA insertion and alignment limits), the power distribution does not result in violation of this LCO. The limiting safety system settings (LSSS) and this LCO are based on the accident analyses (Refs. 1 and 2), so that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences (AOOs), and the limits of acceptable consequences are not exceeded for other postulated accidents.

Limiting power distribution skewing over time also minimizes the xenon distribution skewing, which is a significant factor in controlling the axial power distribution.

Power distribution is a product of multiple parameters, various combinations of which may produce acceptable power distributions. Operation within the design limits of power distribution is accomplished by generating operating limits on the linear heat rate (LHR) and departure from nucleate boiling (DNB).

BASES

BACKGROUND (continued)

The limits on LHR, Total Planar Radial Peaking Factor (F_{XY}^{T}), F_r^T, T_q, and ASI represent limits within which the LHR algorithms are valid. These limits are obtained directly from the core reload analysis.

Either of the two core power distribution monitoring systems, the Excore Detector Monitoring System or the Incore Detector Monitoring System, provide adequate monitoring of the core power distribution and are capable of verifying that the LHR does not exceed its limits. The Excore Detector Monitoring System performs this function by continuously monitoring the ASI with the OPERABLE quadrant symmetric excore neutron flux detectors and verifying that the ASI is maintained within the allowable limits specified in the COLR.

In conjunction with the use of the Excore Detector Monitoring System and in establishing the ASI limits, the following conditions are assumed:

a. The CEA insertion limits of LCO 3.1.5, "Shutdown CEA Insertion Limits," and LCO 3.1.6, "Regulating CEA Insertion Limits," are satisfied,

b. The T_q restrictions of LCO 3.2.4 are satisfied, and

c. F_{xy}^{T} does not exceed the limits of LCO 3.2.2.

The Incore Detector Monitoring System continuously provides a more direct measure of the peaking factors, and the alarms established for the individual incore detector segments ensure that the peak LHRs are maintained within the limits specified in the COLR. The setpoints for these alarms include tolerances, set in conservative directions, for:

a. A measurement calculational uncertainty factor of 1.062,

b. An engineering uncertainty factor of 1.03,

c. An allowance of 1.002 for axial fuel densification and thermal expansion, and

d. A THERMAL POWER measurement uncertainty factor of 1.02.

BASES

APPLICABLE SAFETY ANALYSES

The fuel cladding must not sustain damage as a result of normal operation (Condition 1) and AOOs (Condition 2) (Ref. 3, GDC 10). The power distribution and CEA insertion and alignment LCOs preclude core power distributions that violate the following fuel design criteria:

a. During a LOCA, peak cladding temperature must not exceed 2200°F (Ref. 4),

b. During a loss of flow accident, there must be at least 95% probability at the 95% confidence level (the 95/95 DNB criterion) that the hot fuel rod in the core does not experience a DNB condition (Ref. 3, GDC 10),

c. During an ejected CEA accident, the fission energy input to the fuel must not exceed 280 cal/gm (Ref. [ ]), and

d. The control rods must be capable of shutting down the reactor with a minimum required SDM with the highest worth control rod stuck fully withdrawn (Ref. 3, GDC 26).

The power density at any point in the core must be limited to maintain the fuel design criteria (Ref. 4). This is accomplished by maintaining the power distribution and reactor coolant conditions so that the peak LHR and DNB parameters are within operating limits supported by the accident analyses (Ref. 1), with due regard for the correlations between measured quantities, the power distribution, and uncertainties in the determination of power distribution.

Fuel cladding failure during a LOCA is limited by restricting the maximum linear heat generation rate so that the peak cladding temperature does not exceed 2200°F (Ref. 4). High peak cladding temperatures are assumed to cause severe cladding failure by oxidation due to a Zircaloy water reaction.

The LCOs governing LHR, ASI, and the Reactor Coolant System ensure that these criteria are met as long as the core is operated within the ASI, F^T_{XY}, and F^T_r limits specified in the COLR, and within the T_q limits. The latter are process variables that characterize the three dimensional power distribution of the reactor core. Operation within the limits for these variables ensures that their actual values are within the range used in the accident analysis.

BASES

APPLICABLE SAFETY ANALYSES (continued)

Fuel cladding damage does not normally occur while at conditions outside the limits of these LCOs during normal operation. Fuel cladding damage could result, however, if an accident or AOO occurs from initial conditions outside the limits of these LCOs. This potential for fuel cladding damage exists because changes in the power distribution cause increased power peaking and correspondingly increased local LHR.

F_r^T satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

The LCO limits for power distribution are based on correlations between power peaking and measured variables used as inputs to LHR and DNB ratio operating limits. The LCO limits for power distribution, except T_q, are provided in the COLR. The limitation on the LHR ensures that, in the event of a LOCA, the peak temperature of the fuel cladding does not exceed 2200°F.

APPLICABILITY

In MODE 1, power distribution must be maintained within the limits assumed in the accident analysis to ensure that fuel damage does not result following an AOO. In other MODES, this LCO does not apply because there is not sufficient THERMAL POWER to require a limit on the core power distribution.

ACTIONS

A.1, A.2, and A.3

A Note modifying Condition A requires Required Actions A.1, A.2, and A.3 to be completed if the Condition is entered. This ensures that corrective action is taken prior to unrestricted operation.

The limitations on F_r^T provided in the COLR ensure that the assumptions used in the analysis for establishing the ASI, LCO, and LSSS remain valid during operation at the various allowable CEA group insertion limits. If F_r^T exceeds its basic limitation, operation may continue under the additional restrictions imposed by the Required Actions (reducing THERMAL POWER, withdrawing CEAs to or beyond the long term steady state insertion limits of LCO 3.1.6, and establishing a revised upper THERMAL POWER limit) because these additional restrictions provide adequate provisions to ensure that the assumptions used in establishing the LHR, LCO, and LSSS remain valid. Six hours to return F_r^T to within its limits by adjusting the ASI limits based on maximum power allowed for F_{XY}^{T} is reasonable and ensures that all CEAs meet the long term steady state insertion limits of LCO 3.1.6.

BASES

ACTIONS (continued)

B.1

If F_r^T cannot be returned to within its limit, THERMAL POWER must be reduced. A change to MODE 2 provides reasonable assurance that the core is operating within its thermal limits and places the core in a conservative condition. The allowed Completion Time of 6 hours is reasonable, based on operating experience, to reach MODE 2 from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.2.3.1

The periodic Surveillance to determine the calculated F_r^T ensures that F_r^T remains within the range assumed in the analysis throughout the fuel cycle. Determining the measured F_r^T once after each fuel loading prior to exceeding 70% RTP ensures that the core is properly loaded.

Performance of the Surveillance every 31 days of accumulated operation in MODE 1 provides reasonable assurance that unacceptable changes in the F^T_r are promptly detected.

The power distribution map can only be obtained after THERMAL POWER exceeds 20% RTP because the incore detectors are not reliable below 20% RTP.

The SR is modified by a Note that requires SR 3.2.3.2 and SR 3.2.3.3 be completed each time SR 3.2.3.1 is completed. This procedure is required because the values computed by these SRs are required to perform this SR.

SR 3.2.3.2 and SR 3.2.3.3

Measuring the values of F_r^T and T_q each time a value of F_r^T is calculated ensures that the calculated value of F_r^T accurately reflects the condition of the core.

The Frequency for these Surveillances is in accordance with the requirements of SR 3.2.3.1 because these SRs provide information to complete SR 3.2.2.1.

BASES

REFERENCES

1. FSAR, Chapter [15].
2. FSAR, Chapter [6].
3. 10 CFR 50, Appendix A.
4. 10 CFR 50.46.

B 3.2 POWER DISTRIBUTION LIMITS

B 3.2.4 AZIMUTHAL POWER TILT (T_q) (Analog)

BASES

BACKGROUND

The purpose of this LCO (AZIMUTHAL POWER TILT (T_q)) is to limit the core power distribution to the initial values assumed in the accident analyses. Operation within the limits imposed by this LCO limits or prevents potential fuel cladding failures that could breach the primary fission product barrier and release fission products to the reactor coolant in the event of a loss of coolant accident (LOCA), loss of flow accident, ejected control element assembly (CEA) accident, or other postulated accident requiring termination by a Reactor Protection System trip function. This LCO limits the amount of damage to the fuel cladding during an accident by ensuring that the plant is operating within acceptable bounding conditions at the onset of a transient.

Methods of controlling the power distribution include:

a. Using CEAs to alter the axial power distribution,

b. Decreasing CEA insertion by boration, thereby improving the radial power distribution, and

c. Correcting off optimum conditions (e.g., a CEA drop or misoperation of the unit) that cause margin degradations.

The core power distribution is controlled so that, in conjunction with other core operating parameters (e.g., CEA insertion and alignment limits), the power distribution does not result in violation of this LCO. The limiting safety system settings and this LCO are based on the accident analyses (Refs. 1 and 2), so that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences (AOOs), and the limits of acceptable consequences are not exceeded for other postulated accidents.

Limiting power distribution skewing over time also minimizes the xenon distribution skewing, which is a significant factor in controlling the axial power distribution.

Power distribution is a product of multiple parameters, various combinations of which may produce acceptable power distributions. Operation within the design limits of power distribution is accomplished by generating operating limits for linear heat rate (LHR) and departure from nucleate boiling (DNB).

BASES

BACKGROUND (continued)

The limits on LHR, Total Planar Radial Peaking Factor (F_{XY}^T), Total Integrated Radial Peaking Factor (F_r^T), T_q, and ASI represent limits within which the LHR algorithms are valid. These limits are obtained directly from the core reload analysis.

Either of the two core power distribution monitoring systems, the Excore Detector Monitoring System or the Incore Detector Monitoring System, provides adequate monitoring of the core power distribution and is capable of verifying that the LCO limits are not exceeded. The Excore Detector Monitoring System performs this function by continuously monitoring ASI with OPERABLE quadrant symmetric excore neutron detectors and by verifying ASI is maintained within the limits specified in the COLR.

In conjunction with the use of the Excore Detector Monitoring System and in establishing the ASI limits, the following assumptions are made:

a. The CEA insertion limits of LCO 3.1.5, "Shutdown CEA Insertion Limits," and LCO 3.1.6, "Regulating CEA Insertion Limits," are satisfied,

b. The T_q restrictions of LCO 3.2.4 are satisfied, and

c. F_{xy}^T does not exceed the limits of LCO 3.2.2.

The Incore Detector Monitoring System continuously provides a more direct measure of the peaking factors, and the alarms that have been established for the individual incore detector segments ensure that the peak LHRs are maintained within the limits specified in the COLR. The setpoints for these alarms include tolerances, set in conservative directions, for:

a. A measurement calculational uncertainty factor of 1.062,

b. An engineering uncertainty factor of 1.03,

c. An allowance of 1.002 for axial fuel densification and thermal expansion, and

d. A THERMAL POWER measurement uncertainty factor of 1.02.

BASES

APPLICABLE SAFETY ANALYSES

The fuel cladding must not sustain damage as a result of normal operation (Condition 1) or AOOs (Condition 2) (Ref. 3, GDC 10). The power distribution and CEA insertion and alignment LCOs preclude core power distributions that violate the following fuel design criteria:

a. During a LOCA, peak cladding temperature must not exceed 2200°F (Ref. 4),

b. During a loss of flow accident, there must be at least 95% probability at the 95% confidence level (the 95/95 DNB criterion) that the hot fuel rod in the core does not experience a DNB condition (Ref. 3, GDC 10),

c. During an ejected CEA accident, the fission energy input to the fuel must not exceed 280 cal/gm (Ref. [ ]), and

d. The control rods must be capable of shutting down the reactor with a minimum required SDM with the highest worth control rod stuck fully withdrawn (Ref. 3, GDC 26).

The power density at any point in the core must be limited to maintain the fuel design criteria (Ref. 4). This process is accomplished by maintaining the power distribution and reactor coolant conditions so that the peak LHR and DNB parameters are within operating limits supported by the accident analysis (Ref. 1) with due regard for the correlations between measured quantities, the power distribution, and uncertainties in determining the power distribution.

Fuel cladding failure during a LOCA is limited by restricting the maximum linear heat generation rate (LHGR) so that the peak cladding temperature does not exceed 2200°F (Ref. 4). High peak cladding temperatures are assumed to cause severe cladding failure by oxidation due to a Zircaloy water reaction.

The LCOs governing LHR, ASI, and the Reactor Coolant System ensure that these criteria are met as long as the core is operated within the ASI, F_{XY}^{T}, and F_r^T limits specified in the COLR, and within the T_q limits. The latter are process variables that characterize the three dimensional power distribution of the reactor core. Operation within the limits for these variables ensures that their actual values are within the range used in the accident analyses.

BASES

APPLICABLE SAFETY ANALYSES (continued)

Fuel cladding damage does not normally occur while the reactor is operating at conditions outside these LCOs during otherwise normal operation. Fuel cladding damage could result, however, if an accident or AOO occurs from initial conditions outside the limits of these LCOs. Changes in the power distribution cause increased power peaking and correspondingly increased local LHRs.

The T_q satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

The power distribution LCO limits are based on correlations between power peaking and the measured variables used as inputs to the LHR and DNB operating limits. The power distribution LCO limits, except T_q, are provided in the COLR. The limits on LHR ensure that in the event of a LOCA, the peak temperature of the fuel cladding does not exceed 2200°F.

APPLICABILITY

In MODE 1 with THERMAL POWER > 50% RTP, T_q must be maintained within the limits assumed in accident analysis to ensure that fuel damage does not result following an AOO. In other MODES, this LCO does not apply because THERMAL POWER is not sufficient to require a limit on T_q.

ACTIONS

A.1 and A.2

If the measured T_q is > [0.03] and < 0.10, the calculation of T_q may be nonconservative. T_q must be restored within 2 hours or F^T_{XY} and F^T_r must be determined to be within the limits of LCO 3.2.2 and LCO 3.2.3, and determined to be within these limits every 8 hours thereafter, as long as T_q is out of limits. Two hours is sufficient time to allow the operator to reposition CEAs, and significant radial xenon redistribution cannot occur within this time. The 8 hour Completion Time ensures changes in F^T_{XY} and F^T_r can be identified before the limits of LCO 3.2.2 and LCO 3.2.3, respectively, are exceeded.

B.1

If Required Actions and associated Completion Times of Condition A are not met, THERMAL POWER must be reduced to ≤ 50% RTP. This requirement provides reasonable assurance that the core is operating within its thermal limits and places the core in a conservative condition. Four hours is a reasonable time to reach 50% RTP in an orderly manner and without challenging plant systems.

BASES

ACTIONS (continued)

C.1, C.2, and C.3

With $T_q > 0.10$, F_{XY}^T and F_r^T must be within their specified limits to ensure that acceptable flux peaking factors are maintained. Based on operating experience, 1 hour is sufficient time for the operator to evaluate these factors. If F_{XY}^T and F_r^T are within limits, operation may proceed for a total of 2 hours after the Condition is entered while attempts are made to restore T_q to within its limit.

If $T_q \leq 0.10$ cannot be achieved, power must be reduced to ≤ 50% RTP within 2 hours. If the tilt is generated due to a CEA misalignment, operating at ≤ 50% RTP allows for the recovery of the CEA. Except as a result of CEA misalignment, $T_q > 0.10$ is not expected; if it occurs, continued operation of the reactor may be necessary to discover the cause of the tilt. If this procedure is followed, operation is restricted to only those conditions required to identify the cause of the tilt. It is necessary to account explicitly for power asymmetries because the radial power peaking factors used in core power distribution calculations are based on an untilted power distribution.

If T_q is not restored to within its limits, the reactor continues to operate with an axial power distribution mismatch. Continued operation in this configuration may induce an axial xenon oscillation that causes increased LHRs when the xenon redistributes. If T_q cannot be restored to within its limits within 2 hours, reactor power must be reduced. Reducing THERMAL POWER to ≤ 50% RTP within 2 hours provides conservative protection from increased peaking due to potential xenon redistribution. The Required Actions are modified by a Note that requires all subsequent actions to be performed once power reduction commences after entering the Condition if T_q is not restored to < 0.10. This procedure ensures corrective action is taken before unrestricted power operation resumes. Following THERMAL POWER reduction to ≤ 50% RTP, T_q must be restored to ≤ [0.03] before THERMAL POWER is increased (Required Action C.3). This Required Action prevents the operator from increasing THERMAL POWER above the conservative limit when the Condition, T_q outside its limits, has existed but allows the unit to continue operation for diagnostic purposes. The Completion Time of Required Action C.3 is

BASES

ACTIONS (continued)

modified with a Note to indicate that the cause of the out of limit condition must be corrected prior to increasing THERMAL POWER. This Note also indicates that subsequent power operation above 50% RTP may proceed provided that the measured T_q is verified ≤ [0.03] at least once per hour for 12 hours, or until verified at 95% RTP. This ensures that the power distribution is responding as predicted. The Completion Time of 12 hours is a historical value that allows an acceptable exit from the LCO after the T_q value is verified acceptable for 12 hours or until 95% RTP is reached.

SURVEILLANCE REQUIREMENTS

SR 3.2.4.1

T_q must be calculated at 12 hour intervals. The 12 hour Frequency prevents significant xenon redistribution between Surveillances.

REFERENCES

1. FSAR, Chapter [15].
2. FSAR, Chapter [6].
3. 10 CFR 50, Appendix A.
4. 10 CFR 50.

B 3.2 POWER DISTRIBUTION LIMITS

B 3.2.5 AXIAL SHAPE INDEX (ASI) (Analog)

BASES

BACKGROUND

The purpose of this LCO (AXIAL SHAPE INDEX (ASI)) is to limit the core power distribution to the initial values assumed in the accident analysis. Operation within the limits imposed by this LCO either limits or prevents potential fuel cladding failures that could breach the primary fission product barrier and release fission products to the reactor coolant in the event of a loss of coolant accident (LOCA), loss of flow accident, ejected control element assembly (CEA) accident, or other postulated accident requiring termination by a Reactor Protection System trip function. This LCO limits the amount of damage to the fuel cladding during an accident by ensuring that the plant is operating within acceptable bounding conditions at the onset of a transient.

Methods of controlling the power distribution include:

a. Using CEAs to alter the axial power distribution,

b. Decreasing CEA insertion by boration, thereby improving the radial power distribution, and

c. Correcting off optimum conditions (e.g., a CEA drop or misoperation of the unit) that cause margin degradations.

The core power distribution is controlled so that, in conjunction with other core operating parameters (e.g., CEA insertion and alignment limits), the power distribution does not result in violation of this LCO. The limiting safety system settings and this LCO are based on the accident analyses (Refs. 1 and 2), so that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences (AOOs), and the limits of acceptable consequences are not exceeded for other postulated accidents.

Limiting power distribution skewing over time also minimizes the xenon distribution skewing, which is a significant factor in controlling the axial power distribution.

Power distribution is a product of multiple parameters, various combinations of which may produce acceptable power distributions. Operation within the design limits of power distribution is accomplished by generating operating limits on linear heat rate (LHR) and departure from nucleate boiling (DNB).

BASES

BACKGROUND (continued)

The limits on LHR, Total Planar Radial Peaking Factor (F_{XY}^{T}), Total Integrated Radial Peaking Factor (F_{r}^{T}), T_q, and ASI represent limits within which the LHR algorithms are valid. These limits are obtained directly from the core reload analysis.

Either of the two core power distribution monitoring systems, the Excore Detector Monitoring System and the Incore Detector Monitoring System, provide adequate monitoring of the core power distribution and are capable of verifying that the LHR does not exceed its limits. The Excore Detector Monitoring System performs this function by continuously monitoring the ASI with the OPERABLE quadrant symmetric excore neutron flux detectors and verifying that the ASI is maintained within the allowable limits specified in the COLR.

In conjunction with the use of the Excore Detector Monitoring System and in establishing the ASI limits, the following conditions are assumed:

a. The CEA insertion limits of LCO 3.1.5, "Shutdown CEA Insertion Limits," and LCO 3.1.6, "Regulating CEA Insertion Limits," are satisfied,

b. The T_q restrictions of LCO 3.2.4 are satisfied, and

c. F_{xy}^{T} does not exceed the limits of LCO 3.2.2.

The Incore Detector Monitoring System continuously provides a more direct measure of the peaking factors, and the alarms that have been established for the individual incore detector segments ensure that the peak LHR is maintained within the limits specified in the COLR. The setpoints for these alarms include tolerances, set in conservative directions, as follows:

a. A measurement calculational uncertainty factor of 1.062,

b. An engineering uncertainty factor of 1.03,

c. An allowance of 1.002 for axial fuel densification and thermal expansion, and

d. A THERMAL POWER measurement uncertainty factor of 1.02.

BASES

APPLICABLE SAFETY ANALYSES

The fuel cladding must not sustain damage as a result of normal operation (Condition 1) or AOOs (Condition 2) (Ref. 3, GDC 10). The power distribution and CEA insertion and alignment LCOs prevent core power distributions from reaching levels that violate the following fuel design criteria:

a. During a LOCA, peak cladding temperature must not exceed 2200°F (Ref. 4),

b. During a loss of flow accident, there must be at least 95% probability at the 95% confidence level (the 95/95 DNB criterion) that the hot fuel rod in the core does not experience a DNB condition (Ref. 3, GDC 10),

c. During an ejected CEA accident, the fission energy input to the fuel must not exceed 280 cal/gm (Ref. [ ]), and

d. The control rods must be capable of shutting down the reactor with a minimum required SDM with the highest worth control rod stuck fully withdrawn (Ref. 3, GDC 26).

The power density at any point in the core must be limited to maintain the fuel design criteria (Ref. 4). This limitation is accomplished by maintaining the power distribution and reactor coolant conditions so that the peak LHR and DNB parameters are within operating limits supported by the accident analyses (Ref. 1) with due regard for the correlations among measured quantities, the power distribution, and uncertainties in the determination of power distribution.

Fuel cladding failure during a LOCA is limited by restricting the maximum linear heat generation rate so that the peak cladding temperature does not exceed 2200°F (Ref. 4). High peak cladding temperatures are assumed to cause severe cladding failure by oxidation due to a Zircaloy water reaction.

The LCOs governing LHR, ASI, and the Reactor Coolant System ensure that these criteria are met as long as the core is operated within the ASI, F_{XY}^T, and F_r^T limits specified in the COLR, and within the T_q limits. The latter are process variables that characterize the three dimensional power distribution of the reactor core. Operation within the limits for these variables ensures that their actual values are within the ranges used in the accident analyses.

BASES

APPLICABLE SAFETY ANALYSES (continued)

Fuel cladding damage does not normally occur while the reactor is operating at conditions outside these LCOs during normal operation. Fuel cladding damage results, however, when an accident or AOO occurs from initial conditions outside the limits of these LCOs. This potential for fuel cladding damage exists because changes in the power distribution can cause increased power peaking and correspondingly increased local LHRs.

The ASI satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

The power distribution LCO limits are based on correlations between power peaking and certain measured variables used as inputs to the LHR and DNB operating limits. These power distribution LCO limits, except T_q, are provided in the COLR. The limitation on LHR ensures that in the event of a LOCA, the peak temperature of the fuel cladding does not exceed 2200°F.

The limitation on ASI, along with the limitations of LCO 3.3.1, "Reactor Protection System Instrumentation," represents a conservative envelope of operating conditions consistent with the assumptions that have been analytically demonstrated adequate for maintaining an acceptable minimum DNBR throughout all AOOs. Of these, the loss of flow transient is the most limiting. Operation of the core with conditions within the specified limits ensures that an acceptable minimum margin from DNB conditions is maintained in the event of any AOO, including a loss of flow transient.

APPLICABILITY

In MODE 1 with THERMAL POWER > 20% RTP, power distribution must be maintained within the limits assumed in the accident analyses to ensure that fuel damage does not result following an AOO. In other MODES, this LCO does not apply because THERMAL POWER is not sufficient to require a limit on the core power distribution. Below 20% RTP the incore detector accuracy is not reliable.

ACTIONS

A.1

Operating the core within ASI limits specified in the COLR and within the limits of LCO 3.3.1 ensures an acceptable margin for DNB and for maintaining local power density in the event of an AOO. Maintaining ASI within limits also ensures that the limits of 10 CFR 50.46 are not exceeded during accidents. The Required Actions to restore ASI must be completed within 2 hours to limit the duration the plant is operated outside the initial conditions assumed in the accident analyses. In addition, this Completion Time is sufficiently short that the xenon distribution in the core cannot change significantly.

BASES

ACTIONS (continued)

B.1

If the ASI cannot be restored to within its specified limits, or ASI cannot be determined because of Excore Detector Monitoring System inoperability, core power must be reduced. Reducing THERMAL POWER to ≤ 20% RTP provides reasonable assurance that the core is operating farther from thermal limits and places the core in a conservative condition. Four hours is a reasonable amount of time, based on operating experience, to reduce THERMAL POWER to ≤ 20% RTP in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.2.5.1

Verifying that the ASI is within the specified limits provides reasonable assurance that the core is not approaching DNB conditions. A Frequency of 12 hours is adequate for the operator to identify trends in conditions that result in an approach to the ASI limits, because the mechanisms that affect the ASI, such as xenon redistribution or CEA drive mechanism malfunctions, cause the ASI to change slowly and should be discovered before the limits are exceeded.

REFERENCES

1. FSAR, Chapter [15].
2. FSAR, Chapter [6].
3. 10 CFR 50, Appendix A.
4. 10 CFR 50.46.

B 3.2 POWER DISTRIBUTION LIMITS

B 3.2.1 Linear Heat Rate (LHR) (Digital)

BASES

BACKGROUND

The purpose of this LCO is to limit the core power distribution to the initial values assumed in the accident analyses. Operation within the limits imposed by this LCO limits or prevents potential fuel cladding failures that could breach the primary fission product barrier and release fission products to the reactor coolant in the event of a loss of coolant accident (LOCA), loss of flow accident, ejected control element assembly (CEA) accident, or other postulated accident requiring termination by a Reactor Protection System (RPS) trip function. This LCO limits the damage to the fuel cladding during an accident by ensuring that the plant is operating within acceptable bounding conditions at the onset of a transient.

Methods of controlling the power distribution include:

a. Using full or part length CEAs to alter the axial power distribution,

b. Decreasing CEA insertion by boration, thereby improving the radial power distribution, and

c. Correcting off optimum conditions (e.g., a CEA drop or misoperation of the unit) that cause margin degradations.

The core power distribution is controlled so that, in conjunction with other core operating parameters (e.g., CEA insertion and alignment limits), the power distribution does not result in violation of this LCO. The limiting safety system settings and this LCO are based on the accident analyses (Refs. 1 and 2), so that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences (AOOs), and the limits of acceptable consequences are not exceeded for other postulated accidents.

Limiting power distribution skewing over time also minimizes xenon distribution skewing, which is a significant factor in controlling the axial power distribution.

Power distribution is a product of multiple parameters, various combinations of which may produce acceptable power distributions. Operation within the design limits of power distribution is accomplished by generating operating limits on the LHR and departure from nucleate boiling (DNB).

BASES

BACKGROUND (continued)

Proximity to the DNB condition is expressed by the departure from nucleate boiling ratio (DNBR), defined as the ratio of the cladding surface heat flux required to cause DNB to the actual cladding surface heat flux. The minimum DNBR value during both normal operation and AOOs is calculated by the CE-1 Correlation (Ref. 3) and corrected for such factors as rod bow and grid spacers. It is accepted as an appropriate margin to DNB for all operating conditions.

There are two systems that monitor core power distribution online: the Core Operating Limit Supervisory System (COLSS) and the core protection calculators (CPCs). The COLSS and CPCs that monitor the core power distribution are capable of verifying that the LHR and the DNBR do not exceed their limits. The COLSS performs this function by continuously monitoring the core power distribution and calculating core power operating limits corresponding to the allowable peak LHR and DNBR. The CPCs perform this function by continuously calculating an actual value of DNBR and local power density (LPD) for comparison with the respective trip setpoints.

A DNBR penalty factor is included in both the COLSS and CPC DNBR calculations to accommodate the effects of rod bow. The amount of rod bow in each assembly is dependent upon the average burnup experienced by that assembly. Fuel assemblies that incur higher than average burnup experience a greater magnitude of rod bow. Conversely, fuel assemblies that receive lower than average burnup experience less rod bow. In design calculations for a reload core, each batch of fuel is assigned a penalty applied to the maximum integrated planar radial power peak of the batch. This penalty is correlated with the amount of rod bow determined from the maximum average assembly burnup of the batch. A single net penalty for the COLSS and CPCs is then determined from the penalties associated with each batch that comprises a core reload, accounting for the offsetting margins due to the lower radial power peaks in the higher burnup batches.

The COLSS indicates continuously to the operator how far the core is from the operating limits and provides an audible alarm if an operating limit is exceeded. Such a condition signifies a reduction in the capability of the plant to withstand an anticipated transient, but does not necessarily imply an immediate violation of fuel design limits. If the margin to fuel design limits continues to decrease, the RPS ensures that the specified acceptable fuel design limits are not exceeded during AOOs by initiating reactor trips.

BASES

BACKGROUND (continued)

The COLSS continually generates an assessment of the calculated margin for specified LHR and DNBR limits. The data required for these assessments include measured incore neutron flux, CEA positions, and Reactor Coolant System (RCS) inlet temperature, pressure, and flow.

In addition to the monitoring performed by the COLSS, the RPS (via the CPCs) continually infers the core power distribution and thermal margins by processing reactor coolant data, signals from excore neutron flux detectors, and input from redundant reed switch assemblies that indicate CEA positions. In this case, the CPCs assume a minimum core power of 20% RTP because the power range excore neutron flux detecting system is inaccurate below this power level. If power distribution or other parameters are perturbed as a result of an AOO, the high LPD or low DNBR trips in the RPS initiate a reactor trip prior to the exceeding of fuel design limits.

The LHR and DNBR algorithms are valid within the limits on ASI, F_{xy} and T_Q. These limits are obtained directly from initial core or reload analysis.

APPLICABLE SAFETY ANALYSES

The fuel cladding must not sustain damage as a result of normal operation or AOOs (Ref. 4).

The power distribution and CEA insertion and alignment LCOs prevent core power distributions from reaching levels that violate the following fuel design criteria:

a. During a LOCA, peak cladding temperature must not exceed 2200°F (Ref. 5),

b. During a loss of flow accident, there must be at least 95% probability at the 95% confidence level (the 95/95 DNB criterion) that the hot fuel rod in the core does not experience a DNB condition (Ref. 4),

c. During an ejected CEA accident, the fission energy input to the fuel must not exceed 280 cal/gm (Ref. [ ]), and

d. The control rods must be capable of shutting down the reactor with a minimum required SDM with the highest worth control rod stuck fully withdrawn (GDC 26, Ref. [ ]).

BASES

APPLICABLE SAFETY ANALYSES (continued)

The power density at any point in the core must be limited to maintain the fuel design criteria (Refs. 4 and 5). This is accomplished by maintaining the power distribution and reactor coolant conditions so that the peak LHR and DNB parameters are within operating limits supported by the accident analyses (Ref. 1) with due regard for the correlations between measured quantities, the power distribution, and uncertainties in determining the power distribution.

Fuel cladding failure during a LOCA is limited by restricting the maximum linear heat generation rate so that the peak cladding temperature does not exceed 2200°F (Ref. 5). Peak cladding temperatures exceeding 2200°F cause severe cladding failure by oxidation due to a Zircaloy water reaction.

The LCOs governing the LHR, ASI, and RCS ensure that these criteria are met as long as the core is operated within the ASI and F_{xy} limits specified in the COLR, and within the T_Q limits. The latter are process variables that characterize the three dimensional power distribution of the reactor core.

Operation within the limits for these variables ensures that their actual values are within the ranges used in the accident analyses.

Fuel cladding damage does not normally occur from conditions outside the limits of these LCOs during normal operation. However, fuel cladding damage could result if an accident or AOO occurs from initial conditions outside the limits of these LCOs. This potential for fuel cladding damage exists because changes in the power distribution can cause increased power peaking and can correspondingly increase local LHR.

The LHR satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

The power distribution LCO limits are based on correlations between power peaking and certain measured variables used as inputs to the LHR and DNBR operating limits. The power distribution LCO limits are provided in the COLR. The limitation on LHR ensures that in the event of a LOCA the peak temperature of the fuel cladding does not exceed 2200°F.

BASES

APPLICABILITY

Power distribution is a concern any time the reactor is critical. The power distribution LCOs, however, are only applicable in MODE 1 above 20% RTP. The reasons these LCOs are not applicable below 20% RTP are:

a. The incore neutron detectors that provide input to the COLSS, which then calculates the operating limits, are inaccurate due to the poor signal to noise ratios at relatively low core power levels and

b. As a result of this inaccuracy, the CPCs assume minimum core power of 20% RTP when generating LPD and DNBR trip signals. When core power is below 20% RTP, the core is operating well below its thermal limits and the resultant CPC calculated LPD and DNBR trips are highly conservative.

ACTIONS

A.1

Operation at or below the COLSS calculated power limit based on the LHR ensures that the LHR limit is not exceeded. If the COLSS calculated core power limit based on the LHR exceeds the operating limit, restoring the LHR to within limit in 1 hour ensures that prompt action is taken to reduce LHR to below the specified limit. One hour is a reasonable time to return LHR to within limits when the limit is exceeded without a trip due to events such as a dropped CEA or an axial xenon oscillation.

B.1, B.2.1, and B.2.2

If the COLSS is not available the OPERABLE LPD channels are monitored to ensure that the LHR limit is not exceeded. Operation within this limit ensures that in the event of a LOCA the fuel cladding temperature does not exceed 2200°F. Four hours is allowed for restoring the LHR limit to within the region of acceptable operation. This duration is reasonable because the COLSS allows the plant to operate with less LHR margin (closer to the LHR limit than when monitoring the CPCs).

When operating with the COLSS out of service there is a possibility of a slow undetectable transient that degrades the LHR slowly over the 4 hour period and is then followed by an AOO or an accident. To remedy this, the CPC calculated values of LHR are monitored every 15 minutes when the COLSS is out of service. The 15 minute Frequency is adequate to allow the operator to identify an adverse trend in conditions that could result in an approach to the LHR limit. Also, a maximum allowable

BASES

ACTIONS (continued)

change in the CPC calculated LHR ensures that further degradation requires the operators to take immediate action to restore LHR to within limits or reduce reactor power to comply with the Technical Specifications (TS). With an adverse trend, 1 hour is allowed for restoring LHR to within limits if the COLSS is not restored to OPERABLE status. Implementation of this requirement ensures that reductions in core thermal margin are quickly detected, and if necessary, results in a decrease in reactor power and subsequent compliance with the existing COLSS out of service TS limits.

With no adverse trend, 4 hours is allowed to restore the LHR to within limits if the COLSS is not restored to OPERABLE status. This duration is reasonable because the Frequency of the CPC determination of LHR is increased and if operation is maintained steady, the likelihood of exceeding the LHR limit during this period is not increased. The likelihood of induced reactor transients from an early power reduction is also decreased.

C.1

If the LHR cannot be returned to within its limit or the LHR cannot be determined because of the COLSS and CPC inoperability, core power must be reduced. Reduction of core power to < 20% RTP ensures that the core is operating within its thermal limits and places the core in a conservative condition based on the trip setpoints generated by the CPCs, which assume a minimum core power of 20% RTP. The allowed Completion Time of 6 hours is reasonable, based on operating experience, to reach 20% RTP in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.2.1.1

With the COLSS out of service, the operator must monitor the LHR with each OPERABLE local power density channel. A 2 hour Frequency is sufficient to allow the operator to identify trends that would result in an approach to the LHR limits.

This SR is modified by a Note that states that the SR is only required to be met when the COLSS is out of service. Continuous monitoring of the LHR is provided by the COLSS, which calculates core power and core power operating limits based on the LHR and continuously displays these limits to the operator. A COLSS margin alarm is annunciated in the event that the THERMAL POWER exceeds the core power operating limit based on LHR.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.2.1.2

Verification that the COLSS margin alarm actuates at a THERMAL POWER level equal to or less than the core power operating limit based on the LHR in units of kilowatts per foot ensures the operator is alerted when conditions approach the LHR operating limit.

The 31 day Frequency for performance of this SR is consistent with the historical testing frequency of reactor protection and monitoring systems. The Surveillance Frequency for testing protection systems was extended to 92 days by CEN 327. Monitoring systems were not addressed in CEN 327; therefore, this Frequency remains at 31 days.

REFERENCES

1. FSAR, Section [15].
2. FSAR, Section [6].
3. CE-1 Correlation for DNBR.
4. 10 CFR 50.46, Appendix A, GDC 10.
5. 10 CFR 50.46.

B 3.2 POWER DISTRIBUTION LIMITS

B 3.2.2 Planar Radial Peaking Factors (F_{xy}) (Digital)

BASES

BACKGROUND

The purpose of this LCO is to limit the core power distribution to the initial values assumed in the accident analyses. Operation within the limits imposed by this LCO either limits or prevents potential fuel cladding failures that could breach the primary fission product barrier and release fission products to the reactor coolant in the event of a loss of coolant accident (LOCA), loss of flow accident, ejected control element assembly (CEA) accident, or other postulated accident requiring termination by a Reactor Protection System (RPS) trip function. This LCO limits damage to the fuel cladding during an accident by ensuring that the plant is operating within acceptable conditions at the onset of a transient.

Methods of controlling the power distribution include:

a. Using full or part length CEAs to alter the axial power distribution,

b. Decreasing CEA insertion by boration, thereby improving the radial power distribution, and

c. Correcting off optimum conditions (e.g., a CEA drop or misoperation of the unit) that cause margin degradations.

The core power distribution is controlled so that, in conjunction with other core operating parameters (CEA insertion and alignment limits), the power distribution does not result in violation of this LCO. Limiting safety system settings and this LCO are based on the accident analyses (Refs. 1 and 2), so that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences (AOOs), and the limits of acceptable consequences are not exceeded for other postulated accidents.

Limiting power distribution skewing over time also minimizes xenon distribution skewing, which is a significant factor in controlling axial power distribution. Power distribution is a product of multiple parameters, various combinations of which may produce acceptable power distributions. Operation within the design limits of power distribution is accomplished by generating operating limits on linear heat rate (LHR) and departure from nucleate boiling (DNB).

BASES

BACKGROUND (continued)

Proximity to the DNB condition is expressed by the departure from nucleate boiling ratio (DNBR), defined as the ratio of the cladding surface heat flux required to cause DNB to the actual cladding surface heat flux. The minimum DNBR value during both normal operation and AOOs is [ ] as calculated by the CE-1 Correlation (Ref. 3) and corrected for such factors as rod bow and grid spacers, and it is accepted as an appropriate margin to DNB for all operating conditions.

There are two systems that monitor core power distribution online: the Core Operating Limit Supervisory System (COLSS) and the core protection calculators (CPCs). The COLSS and CPCs that monitor the core power distribution are capable of verifying that the LHR and the DNBR do not exceed their limits. The COLSS performs this function by continuously monitoring the core power distribution and calculating core power operating limits corresponding to the allowable peak LHR and DNBR values. The CPCs perform this function by continuously calculating actual values of DNBR and local power density (LPD) for comparison with the respective trip setpoints.

DNBR penalty factors are included in both the COLSS and CPC DNBR calculations to accommodate the effects of rod bow. The amount of rod bow in each assembly is dependent upon the average burnup experienced by that assembly. Fuel assemblies that incur higher than average burnup experience greater rod bow. Conversely, fuel assemblies that receive lower than average burnup experience less rod bow. In design calculations for a reload core, each batch of fuel is assigned a penalty applied to the maximum integrated planar radial power peak of the batch. This penalty is correlated with the amount of rod bow determined from the maximum average assembly burnup of the batch. A single net penalty for the COLSS and CPCs is then determined from the penalties associated with each batch that comprises a core reload, accounting for the offsetting margins due to the lower radial power peaks in the higher burnup batches.

The COLSS indicates continuously to the operator how near the core is to the operating limits and provides an audible alarm if an operating limit is exceeded. Such a condition signifies a reduction in the capability of the plant to withstand an anticipated transient, but does not necessarily imply an immediate violation of fuel design limits. If the margin to fuel design limits continues to decrease, the RPS ensures that the specified acceptable fuel design limits are not exceeded for AOOs by initiating a reactor trip.

BASES

BACKGROUND (continued)

The COLSS continually generates an assessment of the calculated margin for LHR and DNBR specified limits. The data required for these assessments include measured incore neutron flux, CEA positions, and Reactor Coolant System (RCS) inlet temperature, pressure, and flow.

In addition to monitoring performed by the COLSS, the RPS (via the CPCs) continually infers the core power distribution and thermal margins by processing reactor coolant data, signals from excore neutron flux detectors, and input from redundant reed switch assemblies that indicates CEA position. In this case, the CPCs assume a minimum core power of 20% RTP. This threshold is set at 20% RTP because the power range excore neutron flux detecting system is inaccurate below this power level. If power distribution or other parameters are perturbed as a result of an AOO, the high LPD or low DNBR trips in the RPS initiate a reactor trip before fuel design limits are exceeded.

The limits on ASI, F_{xy}, and T_Q represent limits within which the LHR and DNBR algorithms are valid. These limits are obtained directly from the initial core or reload analysis.

APPLICABLE SAFETY ANALYSES

The fuel cladding must not sustain damage as a result of normal operation or AOOs (Ref. 4). The power distribution and CEA insertion and alignment LCOs prevent core power distributions from reaching levels that violate the following fuel design criteria:

a. During a LOCA, peak cladding temperature must not exceed 2200°F (Ref. 5),

b. During a loss of flow accident, there must be at least 95% probability at the 95% confidence level (the 95/95 DNB criterion) that the hot fuel rod in the core does not experience a DNB condition (Ref. 4),

c. During an ejected CEA accident, the fission energy input to the fuel must not exceed 280 cal/gm (Ref. [ ]), and

d. The control rods must be capable of shutting down the reactor with a minimum required SDM with the highest worth control rod stuck fully withdrawn (GDC 26, Ref. [ ]).

The power density at any point in the core must be limited to maintain the fuel design criteria (Refs. 4 and 5). This result is accomplished by maintaining the power distribution and reactor coolant conditions so that the peak LHR and DNB parameters are within operating limits supported by the accident analyses (Ref. 1) with due regard for the correlations between measured quantities, the power distribution, and the uncertainties in the determination of power distribution.

BASES

APPLICABLE SAFETY ANALYSES (continued)

Fuel cladding failure during a LOCA is limited by restricting the maximum linear heat generation rate so that the peak cladding temperature does not exceed 2200°F (Ref. 5). Peak cladding temperatures exceeding 2200°F cause severe cladding failure by oxidation due to a Zircaloy water reaction.

The LCOs governing LHR, ASI, and RCS ensure that these criteria are met as long as the core is operated within the ASI and F_{xy} limits specified in the COLR, and within the T_Q limits. The latter are process variables that characterize the three dimensional power distribution of the reactor core. Operation within the limits for these variables ensures that their actual values are within the ranges used in the accident analyses.

Fuel cladding damage does not normally occur because of conditions outside the limits of these LCOs for ASI, F_{xy}, and T_Q during normal operation. However, fuel cladding damage results if an accident or AOO occurs from initial conditions outside the limits of these LCOs. This potential for fuel cladding damage exists because changes in the power distribution can cause increased power peaking and correspondingly increased LHR.

F_{xy} satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

The power distribution LCO limits are based on correlations between power peaking and certain measured variables used as inputs to the LHR and DNBR operating limits. The power distribution LCO limits are provided in the COLR.

Limiting of the calculated Planar Radial Peaking Factors (F_{XY}^{C}) used in the COLSS and CPCs to values equal to or greater than the measured Planar Radial Peaking Factors (F_{XY}^{M}) ensures that the limits calculated by the COLSS and CPCs remain valid.

APPLICABILITY

Power distribution is a concern any time the reactor is critical. The power distribution LCOs, however, are only applicable in MODE 1 above 20% RTP. The reasons these LCOs are not applicable below 20% RTP are:

a. The incore neutron detectors that provide input to the COLSS, which then calculates the operating limits, are inaccurate because of the poor signal to noise ratio that they experience at relatively low core power levels and

BASES

APPLICABILITY (continued)

b. As a result of this inaccuracy, the CPCs assume a minimum core power of 20% RTP when generating the LPD and DNBR trip signals. When the core power is below 20% RTP, the core is operating well below its thermal limits, and the resultant CPC calculated LPD and DNBR trips are highly conservative.

ACTIONS

A.1.1 and A.1.2

When the F_{XY}^{M} values exceed the F_{XY}^{C} values used in the COLSS and CPCs, nonconservative operating limits and trip setpoints may be calculated. In this case, action must be taken to ensure that the COLSS operating limits and CPC trip setpoints remain valid with respect to the accident analysis. The operator can do this by performing the Required Actions A.1.1 and A.1.2. The 6 hour Completion Time provides the time required to calculate the required multipliers and make the necessary adjustments to the CPC addressable constants. During this period the DNBR and LHR setpoints may be slightly nonconservative but DNBR and LHR are still within limits. Therefore, 6 hours is an acceptable Completion Time to perform these actions considering the low probability of an accident occurring during this time period.

A.2

As an alternative to Required Actions A.1.1 and A.1.2, the operator may adjust the affected values of F_{XY}^{C} used in the COLSS and CPCs to values $\geq F_{XY}^{M}$. The 6 hour Completion Time provides the time required to calculate the required multipliers and make the necessary adjustments to the CPC addressable constants. During this period the DNBR and LHR setpoints may be slightly nonconservative but DNBR and LHR are still within limits. Therefore, 6 hours is an acceptable Completion Time to perform these actions considering the low probability of an accident occurring during this time period.

BASES

ACTIONS (continued)

A.3

If Required Actions A.1.1 and A.1.2 or A.2 cannot be accomplished within 6 hours, the core power must be reduced. Reduction to 20% RTP or less ensures that the core is operating within the specified thermal limits and places the core in a conservative condition based on the trip setpoints generated by the COLSS and CPC operating limits; these limits are established assuming a minimum core power of 20% RTP. Six hours is a reasonable time to reach 20% RTP in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.2.2.1

This periodic Surveillance is for determining, using the Incore Detector System, that F_{XY}^{M} values are ≤ F_{XY}^{C} values used in the COLSS and CPCs. It ensures that the F_{XY}^{C} values used remain valid throughout the fuel cycle. A Frequency of 31 EFPD is acceptable because the power distribution changes only slightly with the amount of fuel burnup. Determining the F_{XY}^{M} values after each fuel loading when THERMAL POWER is > 40% RTP, but prior to its exceeding 70% RTP, ensures that the core is properly loaded.

REFERENCES

1. FSAR, Section [15].
2. FSAR, Section [6].
3. CE-1 Correlation for DNBR.
4. 10 CFR 50.46, Appendix A, GDC 10.
5. 10 CFR 50.46.

B 3.2 POWER DISTRIBUTION LIMITS

B 3.2.3 AZIMUTHAL POWER TILT (T_Q) (Digital)

BASES

BACKGROUND

The purpose of this LCO is to limit the core power distribution to the initial values assumed in the accident analyses. Operation within the limits imposed by this LCO either limits or prevents potential fuel cladding failures that could breach the primary fission product barrier and release fission products to the reactor coolant in the event of a loss of coolant accident (LOCA), loss of flow accident, ejected control element assembly (CEA) accident, or other postulated accident requiring termination by a Reactor Protection System (RPS) trip function. This LCO limits the amount of damage to the fuel cladding during an accident by ensuring that the plant is operating within acceptable conditions at the onset of a transient.

Methods of controlling the power distribution include:

a. Using full or part length CEAs to alter the axial power distribution,

b. Decreasing CEA insertion by boration, thereby improving the radial power distribution, and

c. Correcting off optimum conditions, (e.g., a CEA drop or misoperation of the unit) that cause margin degradations.

The core power distribution is controlled so that, in conjunction with other core operating parameters (e.g., CEA insertion and alignment limits), the power distribution does not result in violation of this LCO. The limiting safety system settings and this LCO are based on the accident analyses (Refs. 1 and 2), so that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences (AOOs) and the limits of acceptable consequences are not exceeded for other postulated accidents.

Limiting power distribution skewing over time also minimizes xenon distribution skewing, which is a significant factor in controlling axial power distribution.

Power distribution is a product of multiple parameters, various combinations of which may produce acceptable power distributions. Operation within the design limits of power distribution is accomplished by generating operating limits on the linear heat rate (LHR) and the departure from nucleate boiling (DNB).

BASES

BACKGROUND (continued)

Proximity to the DNB condition is expressed by the departure from nucleate boiling ratio (DNBR), defined as the ratio of the cladding surface heat flux required to cause DNB to the actual cladding surface heat flux. The minimum DNBR value during both normal operation and AOOs is calculated by the CE-1 Correlation (Ref. 3) and corrected for such factors as rod bow and grid spacers, and it is accepted as an appropriate margin to DNB for all operating conditions.

There are two systems that monitor core power distribution online: the Core Operating Limit Supervisory System (COLSS) and the core protection calculators (CPCs). The COLSS and CPCs that monitor the core power distribution are capable of verifying that the LHR and the DNBR do not exceed their limits. The COLSS performs this function by continuously monitoring the core power distribution and calculating core power operating limits corresponding to the allowable peak LHR and DNBR. The CPCs perform this function by continuously calculating actual values of DNBR and local power density (LPD) for comparison with the respective trip setpoints.

A DNBR penalty factor is included in the COLSS and CPC DNBR calculation to accommodate the effects of rod bow. The amount of rod bow in each assembly is dependent upon the average burnup experienced by the assembly. Fuel assemblies that incur higher than average burnup experience greater magnitude of rod bow. Conversely, fuel assemblies that receive lower than average burnup experience less rod bow. In design calculations for a reload core, each batch of fuel is assigned a penalty applied to the maximum integrated planar radial power peak of the batch. This penalty is correlated with the amount of rod bow that is determined from the maximum average assembly burnup of the batch. A single net penalty for the COLSS and CPCs is then determined from the penalties associated with each batch that comprises a core reload, accounting for the offsetting margins caused by the lower radial power peaks in the higher burnup batches.

The COLSS indicates continuously to the operator how far the core is from the operating limits and provides an audible alarm if an operating limit is exceeded. Such a condition signifies a reduction in the capability of the plant to withstand an anticipated transient, but does not necessarily imply an immediate violation of fuel design limits. If the margin to fuel design limits continues to decrease, the RPS ensures that the specified acceptable fuel design limits are not exceeded for AOOs by initiating a reactor trip.

BASES

BACKGROUND (continued)

The COLSS continually generates an assessment of the calculated margin for LHR and DNBR specified limits. The data required for these assessments include measured incore neutron flux data, CEA positions, and Reactor Coolant System (RCS) inlet temperature, pressure, and flow.

In addition to the monitoring performed by the COLSS, the RPS (via the CPCs) continually infers the core power distribution and thermal margins by processing reactor coolant data, signals from excore neutron flux detectors, and input from redundant reed switch assemblies that indicates CEA position. In this case, the CPCs assume a minimum core power of 20% RTP. This threshold is set at 20% RTP because the power range excore neutron flux detection system is inaccurate below this power level. If power distribution or other parameters are perturbed as a result of an AOO, the high local power density or low DNBR trips in the RPS initiate a reactor trip prior to exceeding fuel design limits.

The limits on the ASI, F_{xy}, and T_Q represent limits within which the LHR and DNBR algorithms are valid. These limits are obtained directly from the initial core or reload analysis.

APPLICABLE SAFETY ANALYSES

The fuel cladding must not sustain damage as a result of operation and AOOs (Ref. 4). The power distribution and CEA insertion and alignment LCOs preclude core power distributions that violate the following fuel design criteria:

a. During a LOCA, peak cladding temperature must not exceed 2200°F (Ref. 5),

b. During a loss of flow accident, there must be at least 95% probability at the 95% confidence level (the 95/95 DNB criterion) that the hot fuel rod in the core does not experience a DNB condition (Ref. 4),

c. During a CEA ejection accident, the fission energy input to the fuel must not exceed 280 cal/gm (Ref. [5]), and

d. The control rods must be capable of shutting down the reactor with a minimum required SDM with the highest worth control rod stuck fully withdrawn (Ref. [6]).

BASES

APPLICABLE SAFETY ANALYSES (continued)

The power density at any point in the core must be limited to maintain the fuel design criteria (Ref. 1). This result is accomplished by maintaining the power distribution and reactor coolant conditions so that the peak LHR and DNB parameters are within operating limits supported by the accident analysis (Ref. 2) with due regard for the correlations between measured quantities, the power distribution, and uncertainties in the determination of power distribution.

Fuel cladding failure during a LOCA is limited by restricting the maximum linear heat generation rate (LHGR) so that the peak cladding temperature does not exceed 2200°F (Ref. 1). Peak cladding temperatures exceeding 2200°F cause severe cladding failure by oxidation due to a Zircaloy water reaction.

The LCOs governing LHR, ASI, and RCS ensure that these criteria are met as long as the core is operated within the ASI and F_{xy} limits specified in the COLR, and within the T_Q limits. The latter are process variables that characterize the three dimensional power distribution of the reactor core. Operation within the limits of these variables ensures that their actual values are within the range used in the accident analyses.

Fuel cladding damage does not normally occur from conditions outside the limits of these LCOs during normal operation. However, fuel cladding damage could result if an accident or AOO occurs due to initial conditions outside the limits of these LCOs. The potential for fuel cladding damage exists because changes in the power distribution can cause increased power peaking and correspondingly increased local LHRs.
T_Q satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

The power distribution LCO limits are based on correlations between power peaking and certain measured variables used as inputs to the LHR and DNBR operating limits. The power distribution LCO limits are provided in the COLR.

The limitations on the T_Q are provided to ensure that design operating margins are maintained. T_Q > 0.10 is not expected. If it occurs, the actions to be taken ensure that operation is restricted to only those conditions required to identify the cause of the tilt. It is necessary to explicitly account for power asymmetries because the radial peaking factors used in the core power distribution calculations are based on an untilted power distribution.

BASES

APPLICABILITY

Power distribution is a concern any time the reactor is critical. The power distribution LCOs, however, are only applicable in MODE 1 above 20% RTP. The reasons these LCOs are not applicable below 20% RTP are:

a. The incore neutron detectors that provide input to the COLSS, which then calculates the operating limits, are inaccurate due to the poor signal to noise ratio that they experience at relatively low core power levels.

b. As a result of this inaccuracy, the CPCs assume a minimum core power of 20% RTP when generating LPD and DNBR trip signals. When the core power is below this level, the core is operating well below its thermal limits and the resultant CPC calculated LPD and DNBR trips are highly conservative.

ACTIONS

A.1 and A.2

If the measured T_Q is greater than the T_Q allowance used in the CPCs but ≤ 0.10, nonconservative trip setpoints may be calculated. Required Action A.1 restores T_Q to within its specified limits by repositioning the CEAs, and the reactor may return to normal operation. A Completion Time of 2 hours is sufficient time to allow the operator to reposition the CEAs because significant radial xenon redistribution does not occur within this time.

If the T_Q cannot be restored within 2 hours, the T_Q allowance in the CPCs must be adjusted, per Required Action A.2, to be equal to or greater than the measured value of T_Q to ensure that the design safety margins are maintained.

B.1, B.2, and B.3

Required Actions B.1, B.2, and B.3 are modified by a Note that requires all subsequent actions be performed if power reduction commences prior to restoring T_Q ≤ 0.10. This requirement ensures that corrective action is taken before unrestricted power operation resumes.

If the measured T_Q > 0.10, THERMAL POWER is reduced to ≤ 50% RTP within 4 hours. The 4 hours allows enough time to take action to restore T_Q prior to reducing power and limits the probability of operation with a power distribution out of limits. Such actions include performing SR 3.2.3.2, which provides a value of T_Q that can be used in subsequent actions.

BASES

ACTIONS (continued)

Also in the case of a tilt generated by a CEA misalignment, the 4 hours allows recovery of the CEA misalignment, because a measured $T_Q > 0.10$ is not expected. If it occurs, continued operation of the reactor may be necessary to discover the cause of the tilt. Operation then is restricted to only those conditions required to identify the cause of the tilt. It is necessary to explicitly account for power asymmetries because the radial power peaking factors used in the core power distribution calculation are based on an untilted power distribution.

If the measured T_Q is not restored to within its specified limits, the reactor continues to operate with an axial power distribution mismatch. Continued operation in this configuration may induce an axial xenon oscillation, which results in increased LHGRs when the xenon redistributes. If the measured T_Q cannot be restored to within its limit within 4 hours, reactor power must be reduced. Reducing THERMAL POWER to < 50% RTP within 4 hours provides an acceptable level of protection from increased power peaking due to potential xenon redistribution while maintaining a power level sufficiently high enough to allow the tilt to be analyzed.

The Linear Power Level - High trip setpoints are reduced to ≤ 55% RTP to ensure that the assumptions of the accident analysis regarding power peaking are maintained. After power has been reduced to ≤ 50% RTP, the rate and magnitude of changes in the core flux are greatly reduced. Therefore, 16 hours is an acceptable time period to allow for reduction of the Linear Power Level - High trip setpoints, Required Action B.2. The 16 hour Completion Time allowed to reduce the Linear Power Level - High trip setpoints is required to perform the actions necessary to reset the trip setpoints.

THERMAL POWER is restricted to 50% RTP until the measured T_Q is restored to within its specified limit by correcting the out of limit condition. This action prevents the operator from increasing THERMAL POWER above the conservative limit when a significant T_Q has existed, but allows the unit to continue operation for diagnostic purposes.

The Completion Time of Required Action B.3 is modified by a Note governing subsequent power increases. After a THERMAL POWER increase following restoration of T_Q, operation may proceed provided the measured T_Q is determined to remain within its specified limit at the increased THERMAL POWER level.

BASES

ACTIONS (continued)

The provision to allow discontinuation of the Surveillance after verifying that $T_Q \leq 0.10$ is within its specified limit at least once per hour for 12 hours or until T_Q is verified to be within its specified limit at a THERMAL POWER ≥ 95% RTP provides an acceptable exit from this action after the measured T_Q has been returned to an acceptable value.

C.1

If the measured T_Q cannot be restored or determined within its specified limit, core power must be reduced. Reduction of core power to < 20% RTP ensures that the core is operating within its thermal limits and places the core in a conservative condition based on the trip setpoints generated by the CPCs, which assume a minimum core power of 20% RTP. Six hours is a reasonable time to reach 20% RTP in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.2.3.1

Continuous monitoring of the measured T_Q by the incore nuclear detectors is provided by the COLSS. A COLSS alarm is annunciated in the event that the measured T_Q exceeds the value used in the CPCs.

With the COLSS out of service, the operator must calculate T_Q and verify that it is within its specified limits. The 12 hour Frequency is sufficient to identify slowly developing T_Q's before they exceed the limits of this LCO. Also, the 12 hour Frequency prevents significant xenon redistribution.

SR 3.2.3.2

Verification that the COLSS T_Q alarm actuates at a value less than the value used in the CPCs ensures that the operator is alerted if T_Q approaches its operating limit. The 31 day Frequency for performance of this SR is consistent with the historical testing frequency of reactor protection and monitoring systems. The Surveillance Frequency for testing protection systems was extended to 92 days by CEN 327. Monitoring systems were not addressed in CEN 327; therefore, this Frequency remains at 31 days.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.2.3.3

Independent confirmation of the validity of the COLSS calculated T_Q ensures that the COLSS accurately identifies T_Q's.

The 31 day Frequency for performance of this SR is consistent with the historical testing frequency of reactor protection and monitoring systems. The Surveillance Frequency for testing protection systems was extended to 92 days by CEN 327. Monitoring systems were not addressed in CEN 327; therefore, this Frequency remains at 31 days.

REFERENCES

1. FSAR, Section [15].
2. FSAR, Section [6].
3. CE-1 Correlation for DNBR.
4. 10 CFR 50.46, Appendix A, GDC 10.
5. 10 CFR 50.46.
6. 10 CFR 50, Appendix A, GDC 26.

B 3.2 POWER DISTRIBUTION LIMITS

B 3.2.4 Departure from Nucleate Boiling Ratio (DNBR) (Digital)

BASES

BACKGROUND

The purpose of this LCO is to limit the core power distribution to the initial value assumed in the accident analyses. Specifically, operation within the limits imposed by this LCO either limits or prevents potential fuel cladding failures that could breach the primary fission product barrier and release fission products to the reactor coolant in the event of a loss of coolant accident (LOCA), loss of flow accident, ejected control element assembly (CEA) accident, or other postulated accident requiring termination by a Reactor Protection System (RPS) trip function. This LCO limits the amount of damage to the fuel cladding during an accident by ensuring that the plant is operating within acceptable conditions at the onset of a transient.

Methods of controlling the power distribution include:

a. Using full or part length CEAs to alter the axial power distribution,

b. Decreasing CEA insertion by boration, thereby improving the radial power distribution, and

c. Correcting off optimum conditions (e.g., a CEA drop or misoperation of the unit) that cause margin degradations.

The core power distribution is controlled so that, in conjunction with other core operating parameters (e.g., CEA insertion and alignment limits), the power distribution does not result in violation of this LCO. The limiting safety system settings and this LCO are based on the accident analysis (Refs. 1 and 2), so that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences (AOOs) and the limits of acceptable consequences are not exceeded for other postulated accidents.

Limiting power distribution skewing over time also minimizes the xenon distribution skewing, which is a significant factor in controlling axial power distribution.

Power distribution is a product of multiple parameters, various combinations of which may produce acceptable power distributions. Operation within the design limits of power distribution is accomplished by generating operating limits on the linear heat rate (LHR) and the departure from nucleate boiling (DNB).

BASES

BACKGROUND (continued)

Proximity to the DNB condition is expressed by the DNBR, defined as the ratio of the cladding surface heat flux required to cause DNB to the actual cladding surface heat flux. The minimum DNBR value during both normal operation and AOOs is [ ] as calculated by the CE-1 Correlation (Ref. 3) and corrected for such factors as rod bows and grid spacers and it is accepted as an appropriate margin to DNB for all operating conditions.

There are two systems that monitor core power distribution online: the Core Operating Limits Supervisory System (COLSS) and the core protection calculators (CPCs). The COLSS and CPCs that monitor the core power distribution are capable of verifying that the LHR and DNBR do not exceed their limits. The COLSS performs this function by continuously monitoring the core power distribution and calculating core power operating limits corresponding to the allowable peak LHR and DNBR. The CPCs perform this function by continuously calculating an actual value of DNBR and LPD for comparison with the respective trip setpoints.

A DNBR penalty factor is included in both the COLSS and CPC DNBR calculation to accommodate the effects of rod bow. The amount of rod bow in each assembly is dependent upon the average burnup experienced by that assembly. Fuel assemblies that incur higher than average burnup experience a greater magnitude of rod bow. Conversely, fuel assemblies that receive lower than average burnup experience less rod bow. In design calculations for a reload core, each batch of fuel is assigned a penalty that is applied to the maximum integrated planar radial power peak of the batch. This penalty is correlated with the amount of rod bow that is determined from the maximum average assembly burnup of the batch. A single net penalty for the COLSS and CPCs is then determined from the penalties associated with each batch that comprises a core reload, accounting for the offsetting margins due to the lower radial power peaks in the higher burnup batches.

The COLSS indicates continuously to the operator how far the core is from the operating limits and provides an audible alarm when an operating limit is exceeded. Such a condition signifies a reduction in the capability of the plant to withstand an anticipated transient, but does not necessarily imply an immediate violation of fuel design limits. If the margin to fuel design limits continues to decrease, the RPS ensures that the specified acceptable fuel design limits are not exceeded during AOOs by initiating a reactor trip.

BASES

BACKGROUND (continued)

The COLSS continually generates an assessment of the calculated margin for LHR and DNBR specified limits. The data required for these assessments include measured incore neutron flux, CEA positions, and Reactor Coolant System (RCS) inlet temperature, pressure, and flow.

In addition to the monitoring performed by the COLSS, the RPS (via the CPCs) continually infers the core power distribution and thermal margins by processing reactor coolant data, signals from excore neutron flux detectors, and input from redundant reed switch assemblies that indicates CEA position. In this case, the CPCs assume a minimum core power of 20% RTP because the power range excore neutron flux detecting system is inaccurate below this power level. If power distribution or other parameters are perturbed as a result of an AOO, the high local power density or low DNBR trips in the RPS initiate a reactor trip prior to the exceeding of fuel design limits.

The limits on ASI, F_{xy}, and T_Q represent limits within which the LHR and DNBR algorithms are valid. These limits are obtained directly from the initial core or reload analysis.

APPLICABLE SAFETY ANALYSES

The fuel cladding must not sustain damage as a result of normal operation or AOOs (Ref. 4). The power distribution and CEA insertion and alignment LCOs prevent core power distributions from reaching levels that violate the following fuel design criteria:

a. During a LOCA, peak cladding temperature must not exceed 2200°F (Ref. 5),

b. During a loss of flow accident, there must be at least 95% probability at the 95% confidence level (the 95/95 DNB criterion) that the hot fuel rod in the core does not experience a DNB condition (Ref. 4),

c. During an ejected CEA accident, the fission energy input to the fuel must not exceed 280 cal/gm (Ref. 6), and

d. The control rods must be capable of shutting down the reactor with a minimum required SDM with the highest worth control rod stuck fully withdrawn (Ref. 7).

The power density at any point in the core must be limited to maintain the fuel design criteria (Ref. 4). This is accomplished by maintaining the power distribution and reactor coolant conditions so that the peak LHR and DNB parameters are within operating limits supported by the accident analyses (Ref. 1) with due regard for the correlations between measured quantities, the power distribution, and uncertainties in the determination of power distribution.

BASES

APPLICABLE SAFETY ANALYSES (continued)

Fuel cladding failure during a LOCA is limited by restricting the maximum linear heat generation rate so that the peak cladding temperature does not exceed 2200°F (Ref. 4). Peak cladding temperatures exceeding 2200°F may cause severe cladding failure by oxidation due to a Zircaloy water reaction.

The LCOs governing LHR, ASI, and RCS ensure that these criteria are met as long as the core is operated within the ASI and F_{xy} limits specified in the COLR, and within the T_Q limits. The latter are process variables that characterize the three dimensional power distribution of the reactor core. Operation within the limits for these variables ensures that their actual values are within the range used in the accident analyses (Ref. 1).

Fuel cladding damage does not normally occur from conditions outside the limits of these LCOs during normal operation. However, fuel cladding damage could result if an accident or AOO occurs from initial conditions outside the limits of these LCOs. This potential for fuel cladding damage exists because changes in the power distribution can cause increased power peaking and correspondingly increased local LHRs.

DNBR satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

The power distribution LCO limits are based on correlations between power peaking and certain measured variables used as inputs to the LHR and DNBR operating limits. The power distribution LCO limits are provided in the COLR.

With the COLSS in service and one or both of the control element assembly calculators (CEACs) OPERABLE, the DNBR will be maintained by ensuring that the core power calculated by the COLSS is equal to or less than the permissible core power operating limit based on DNBR calculated by the COLSS. In the event that the COLSS is in service but neither of the two CEACs is OPERABLE, the DNBR is maintained by ensuring that the core power calculated by the COLSS is equal to or less than a reduced value of the permissible core power operating limit calculated by the COLSS. In this condition, the calculated operating limit must be reduced by the allowance specified in the COLR.

BASES

LCO (continued)

In instances for which the COLSS is out of service and either one or both of the CEACs are OPERABLE, the DNBR is maintained by operating within the acceptable region specified in the COLR as shown in Figure 3.2.4-1, in the COLR, and using any OPERABLE CPC channel. Alternatively, when the COLSS is out of service and neither of the two CEACs is OPERABLE, the DNBR is maintained by operating within the acceptable region specified in the COLR for this condition as shown in Figure 3.2.4-2, in the COLR, and using any OPERABLE CPC channel.

With the COLSS out of service, the limitation on DNBR as a function of the ASI represents a conservative envelope of operating conditions consistent with the analysis assumptions that have been analytically demonstrated adequate to maintain an acceptable minimum DNBR for all AOOs. Of these, the postulated loss of flow transient is the most limiting. Operation of the core with a DNBR at or above this limit ensures that an acceptable minimum DNBR is maintained in the event of a loss of flow transient.

APPLICABILITY

Power distribution is a concern any time the reactor is critical. The power distribution LCOs, however, are only applicable in MODE 1 above 20% RTP. The reasons these LCOs are not applicable below 20% RTP are:

a. The incore neutron detectors that provide input to the COLSS, which then calculates the operating limits, are inaccurate due to the poor signal to noise ratio that they experience at relatively low core power levels.

b. As a result of this inaccuracy, the CPCs assume a minimum core power of 20% RTP when generating the local power density (LPD) and DNBR trip signals. When the core power is below this level, the core is operating well below the thermal limits and the resultant CPC calculated LPD and DNBR trips are highly conservative.

ACTIONS

A.1

Operating at or above the minimum required value of the DNBR ensures that an acceptable minimum DNBR is maintained in the event of a postulated loss of flow transient. If the core power as calculated by the COLSS exceeds the core power limit calculated by the COLSS based on the DNBR, fuel design limits may not be maintained following a loss of flow, and prompt action must be taken to restore the DNBR above its minimum Allowable Value. With the COLSS in service, 1 hour is a reasonable time for the operator to initiate corrective actions to restore the DNBR above its specified limit, because of the low probability of a severe transient occurring in this relatively short time.

BASES

ACTIONS (continued)

B.1, B.2.1, and B.2.2

If the COLSS is not available the OPERABLE DNBR channels are monitored to ensure that the DNBR is not exceeded. Maintaining the DNBR within this specified range ensures that no postulated accident results in consequences more severe than those described in the FSAR, Chapter 15. A 4 hour Frequency is allowed to restore the DNBR limit to within the region of acceptable operation. This Frequency is reasonable because the COLSS allows the plant to operate with less DNBR margin (closer to the DNBR limit) than when monitoring with the CPCs.

When operating with the COLSS out of service there is a possibility of a slow undetectable transient that degrades the DNBR slowly over the 4 hour period and is then followed by an anticipated operational occurrence or an accident. To remedy this, the CPC calculated values of DNBR are monitored every 15 minutes when the COLSS is out of service. The 15 minute Frequency is adequate to allow the operator to identify an adverse trend in conditions that could result in an approach to the DNBR limit. Also, a maximum allowable change in the CPC calculated DNBR ensures that further degradation requires the operators to take immediate action to restore DNBR to within limits or reduce reactor power to comply with the Technical Specifications (TS). With an adverse trend, 1 hour is allowed for restoring DNBR to within limits if the COLSS is not restored to OPERABLE status. Implementation of this requirement ensures that reductions in core thermal margin are quickly detected and, if necessary, results in a decrease in reactor power and subsequent compliance with the existing COLSS out of service TS limits.

With no adverse trend, 4 hours is allowed for restoring the DNBR to within limits if the COLSS is not restored to OPERABLE status. This duration is reasonable because the Frequency of the CPC determination of DNBR has been increased, and, if operation is maintained steady, the likelihood of exceeding the DNBR limit during this period is not increased. The likelihood of induced reactor transients from an early power reduction is also decreased.

BASES

ACTIONS (continued)

C.1

If the DNBR cannot be restored or determined within the allowed times of Conditions A and B, core power must be reduced. Reduction of core power to < 20% RTP ensures that the core is operating within its thermal limits and places the core in a conservative condition based on trip setpoints generated by the CPCs, which assume a minimum core power of 20% RTP.

The allowed Completion Time of 6 hours is reasonable, based on operating experience, to reach 20% RTP from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.2.4.1

With the COLSS out of service, the operator must monitor the DNBR as indicated on any of the OPERABLE DNBR channels of the CPCs to verify that the DNBR is within the specified limits, shown in either Figure 3.2.4-1 or 3.2.4-2 of the COLR, as applicable. A 2 hour Frequency is adequate to allow the operator to identify trends in conditions that would result in an approach to the DNBR limit.

This SR is modified by a Note that states that the SR is only required to be met when the COLSS is out of service. Continuous monitoring of the DNBR is provided by the COLSS, which calculates core power and core power operating limits based on the DNBR and continuously displays these limits to the operator. A COLSS margin alarm is annunciated in the event that the THERMAL POWER exceeds the core power operating limit based on the DNBR.

SR 3.2.4.2

Verification that the COLSS margin alarm actuates at a power level equal to or less than the core power operating limit, as calculated by the COLSS, based on the DNBR, ensures that the operator is alerted when operating conditions approach the DNBR operating limit. The 31 day Frequency for performance of this SR is consistent with the historical testing frequency of reactor protection and monitoring systems. The Surveillance Frequency for testing protection systems was extended to 92 days by CEN 327. Monitoring systems were not addressed in CEN 327; therefore, this Frequency remains at 31 days.

BASES

REFERENCES

1. FSAR, Chapter [15].
2. FSAR, Chapter [6].
3. CE-1 Correlation for DNBR.
4. 10 CFR 50, Appendix A, GDC 10.
5. 10 CFR 50.46.
6. FSAR, Section [ ].
7. 10 CFR 50, Appendix A, GDC 26.

B 3.2 POWER DISTRIBUTION LIMITS

B 3.2.5 AXIAL SHAPE INDEX (ASI) (Digital)

BASES

BACKGROUND

The purpose of this LCO is to limit the core power distribution to the initial values assumed in the accident analysis. Operation within the limits imposed by this LCO either limits or prevents potential fuel cladding failures that could breach the primary fission product barrier and release fission products to the reactor coolant in the event of a loss of coolant accident (LOCA), loss of flow accident, ejected control element assembly (CEA) accident, or other postulated accident requiring termination by a Reactor Protection System (RPS) trip function. This LCO limits the amount of damage to the fuel cladding during an accident by ensuring that the plant is operating within acceptable conditions at the onset of a transient.

Methods of controlling the power distribution include:

a. Using full or part length CEAs to alter the axial power distribution,

b. Decreasing CEA insertion by boration, thereby improving the radial power distribution, and

c. Correcting off optimum conditions (e.g., a CEA drop or misoperation of the unit) that cause margin degradations.

The core power distribution is controlled so that, in conjunction with other core operating parameters (CEA insertion and alignment limits), the power distribution does not result in violation of this LCO. The limiting safety system settings are based on the accident analyses (Refs. 1 and 2), so that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences (AOOs) and the limits of acceptable consequences are not exceeded for other postulated accidents.

Minimizing power distribution skewing over time also minimizes xenon distribution skewing, which is a significant factor in controlling axial power distribution.

Power distribution is a product of multiple parameters, various combinations of which may produce acceptable power distributions. Operation within the design limits of power distribution is accomplished by generating operating limits on the linear heat rate (LHR) and the departure from nucleate boiling (DNB).

BASES

BACKGROUND (continued)

Proximity to the DNB condition is expressed by the departure from nucleate boiling ratio (DNBR), defined as the ratio of the cladding surface heat flux required to cause DNB to the actual cladding surface heat flux. The minimum DNBR value during both normal operation and AOOs is [ ] as calculated by the CE-1 Correlation (Ref. 3), and corrected for such factors as rod bow and grid spacers, and it is accepted as an appropriate margin to DNB for all operating conditions.

There are two systems that monitor core power distribution online: the Core Operating Limit Supervisory System (COLSS) or the core protection calculators (CPCs). The COLSS and CPCs monitor the core power distribution and are capable of verifying that the LHR and DNBR do not exceed their limits. The COLSS performs this function by continuously monitoring the core power distribution and calculating core power operating limits corresponding to the allowable peak LHR and DNBR. The CPCs perform this function by continuously calculating actual values of DNBR and local power density (LPD) for comparison with the respective trip setpoints.

A DNBR penalty factor is included in both the COLSS and CPC DNBR calculations to accommodate the effects of rod bow. The amount of rod bow in each assembly is dependent upon the average burnup experienced by that assembly. Fuel assemblies that incur higher than average burnup experience greater rod bow. Conversely, fuel assemblies that receive lower than average burnup experience less rod bow. In design calculations for a reload core, each batch of fuel is assigned a penalty that is applied to the maximum integrated planar radial power peak of the batch. This penalty is correlated with the amount of rod bow that is determined from the maximum average assembly burnup of the batch. A single net penalty for the COLSS and CPC is then determined from the penalties associated with each batch that comprises a core reload, accounting for the offsetting margins due to the lower radial power peaks in the higher burnup batches.

The COLSS indicates continuously to the operator how far the core is from the operating limits and provides an audible alarm if an operating limit is exceeded. Such a condition signifies a reduction in the capability of the plant to withstand an anticipated transient, but does not necessarily imply an immediate violation of fuel design limits. If the margin to fuel design limits continues to decrease, the RPS ensures that the specified acceptable fuel design limits are not exceeded for AOOs by initiating a reactor trip.

BASES

BACKGROUND (continued)

The COLSS continually generates an assessment of the calculated margin for LHR and DNBR specified limits. The data required for these assessments include measured incore neutron flux, CEA positions, and Reactor Coolant System (RCS) inlet temperature, pressure, and flow.

In addition to the monitoring performed by the COLSS, the RPS (via the CPCs) continually infers the core power distribution and thermal margins by processing reactor coolant data, signals from excore neutron flux detectors, and input from redundant reed switch assemblies that indicates CEA position. In this case, the CPCs assume a minimum core power of 20% RTP because the power range excore neutron flux detecting system is inaccurate below this power level. If power distribution or other parameters are perturbed as a result of an AOO, the high local power density or low DNBR trips in the RPS initiate a reactor trip prior to the exceeding of fuel design limits.

The limits on ASI, F_{xy}, and T_Q represent limits within which the LHR and DNBR algorithms are valid. These limits are obtained directly from the initial core or reload analysis.

APPLICABLE SAFETY ANALYSES

The fuel cladding must not sustain damage as a result of operation or AOOs (Ref. 4). The power distribution and CEA insertion and alignment LCOs prevent core power distributions from reaching levels that violate the following fuel design criteria:

a. During a LOCA, peak cladding temperature must not exceed 2200°F (Ref. 5),

b. During a loss of flow accident, there must be at least 95% probability at the 95% confidence level (the 95/95 DNB criterion) that the hot fuel rod in the core does not experience a DNB condition (Ref. 4),

c. During an ejected CEA accident, the fission energy input to the fuel must not exceed 280 cal/gm (Ref. 6),

d. The control rods must be capable of shutting down the reactor with a minimum required SDM with the highest worth control rod stuck fully withdrawn (Ref. 7).

The power density at any point in the core must be limited to maintain the fuel design criteria (Refs. 4 and 5). This is accomplished by maintaining the power distribution and reactor coolant conditions so that the peak LHR and DNB parameters are within operating limits supported by the accident analyses (Ref. 1) with due regard for the correlations among measured quantities, the power distribution, and uncertainties in the determination of power distribution.

BASES

APPLICABLE SAFETY ANALYSES (continued)

Fuel cladding failure during a LOCA is limited by restricting the maximum linear heat generation rate (LHGR) so that the peak cladding temperature does not exceed 2200°F (Ref. 5). Peak cladding temperatures exceeding 2200°F may cause severe cladding failure by oxidation due to a Zircaloy water reaction.

The LCOs governing LHR, ASI, and RCS ensure that these criteria are met as long as the core is operated within the ASI and F_{xy} limits specified in the COLR, and within the T_Q limits. The latter are process variables that characterize the three dimensional power distribution of the reactor core. Operation within the limits for these variables ensures that their actual values are within the range used in the accident analysis.

Fuel cladding damage does not normally occur from conditions outside these LCOs during normal operation. However, fuel cladding damage results when an accident or AOO occurs due to initial conditions outside the limits of these LCOs. This potential for fuel cladding damage exists because changes in the power distribution can cause increased power peaking and correspondingly increased local LHRs.

The ASI satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

The power distribution LCO limits are based on correlations between power peaking and certain measured variables used as inputs to LHR and DNBR operating limits. The power distribution LCO limits are provided in the COLR.

The limitation on ASI ensures that the actual ASI value is maintained within the range of values used in the accident analysis. The ASI limits ensure that with T_Q at its maximum upper limit, the DNBR does not drop below the DNBR Safety Limit for AOOs.

APPLICABILITY

Power distribution is a concern any time the reactor is critical. The power distribution LCOs, however, are only applicable in MODE 1 above 20% RTP. The reasons these LCOs are not applicable below 20% RTP are:

a. The incore neutron detectors that provide input to the COLSS, which then calculates the operating limits, are inaccurate due to the poor signal to noise ratio that they experience at relatively low core power levels.

BASES

APPLICABILITY (continued)

b. As a result of this inaccuracy, the CPCs assume a minimum core power of 20% RTP when generating the LPD and DNBR trip signals. When the core power is below this level, the core is operating well below the thermal limits and the resultant CPC calculated LPD and DNBR trips are strongly conservative.

ACTIONS

A.1

The ASI limits specified in the COLR ensure that the LOCA and loss of flow accident criteria assumed in the accident analyses remain valid. If the ASI exceeds its limit, a Completion Time of 2 hours is allowed to restore the ASI to within its specified limit. This duration gives the operator sufficient time to reposition the regulating or part length CEAs to reduce the axial power imbalance. The magnitude of any potential xenon oscillation is significantly reduced if the condition is not allowed to persist for more than 2 hours.

B.1

If the ASI is not restored to within its specified limits within the required Completion Time, the reactor continues to operate with an axial power distribution mismatch. Continued operation in this configuration induces an axial xenon oscillation, and results in increased LHGRs when the xenon redistributes. Reducing thermal power to ≤ 20% RTP reduces the maximum LHR to a value that does not exceed the fuel design limits if a design basis event occurs. The allowed Completion Time of 4 hours is reasonable, based on operating experience, to reduce power in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.2.5.1

The ASI can be monitored by both the incore (COLSS) and excore (CPC) neutron detector systems. The COLSS provides the operator with an alarm if an ASI limit is approached.

Verification of the ASI every 12 hours ensures that the operator is aware of changes in the ASI as they develop. A 12 hour Frequency for this Surveillance is acceptable because the mechanisms that affect the ASI, such as xenon redistribution or CEA drive mechanism malfunctions, cause slow changes in the ASI, which can be discovered before the limits are exceeded.

BASES

REFERENCES

1. FSAR, Chapter [15].
2. FSAR, Chapter [6].
3. CE-1 Correlation for DNBR.
4. 10 CFR 50, Appendix A, GDC 10.
5. 10 CFR 50.46.
6. FSAR, Section [ ].
7. 10 CFR 50, Appendix A, GDC 26.

B 3.3 INSTRUMENTATION

B 3.3.1 Reactor Protective System (RPS) Instrumentation - Operating (Analog)

BASES

BACKGROUND

The Reactor Protective System (RPS) initiates a reactor trip to protect against violating the core specified acceptable fuel design limits and breaching the reactor coolant pressure boundary during anticipated operational occurrences (AOOs). By tripping the reactor, the RPS also assists the Engineered Safety Features systems in mitigating accidents.

The protection and monitoring systems have been designed to ensure safe operation of the reactor. This is achieved by specifying limiting safety system settings (LSSS) in terms of parameters directly monitored by the RPS, as well as LCOs on other reactor system parameters and equipment performance.

Technical Specifications are required by 10 CFR 50.36 to contain LSSS defined by the regulation as "...settings for automatic protective devices...so chosen that automatic protective actions will correct the abnormal situation before a Safety Limit (SL) is exceeded." The Analytic Limit is the limit of the process variable at which a safety action is initiated, as established by the safety analysis, to ensure that a SL is not exceeded. Any automatic protection action that occurs on reaching the Analytic Limit therefore ensures that the SL is not exceeded. However, in practice, the actual settings for automatic protective devices must be chosen to be more conservative than the Analytic Limit to account for instrument loop uncertainties related to the setting at which the automatic protective action would actually occur.

The trip setpoint is a predetermined setting for a protective device chosen to ensure automatic actuation prior to the process variable reaching the Analytic Limit and thus ensuring that the SL would not be exceeded. As such, the trip setpoint accounts for uncertainties in setting the device (e.g., calibration), uncertainties in how the device might actually perform (e.g., repeatability), changes in the point of action of the device over time (e.g., drift during surveillance intervals), and any other factors which may influence its actual performance (e.g., harsh accident environments). In this manner, the trip setpoint plays an important role in ensuring that SLs are not exceeded. As such, the trip setpoint meets the definition of an LSSS (Ref. 1) and could be used to meet the requirement that they be contained in the Technical Specifications.

BASES

BACKGROUND (continued)

Technical Specifications contain values related to the OPERABILITY of equipment required for safe operation of the facility. OPERABLE is defined in Technical Specifications as "...being capable of performing its safety function(s)." For automatic protective devices, the required safety function is to ensure that a SL is not exceeded and therefore the LSSS as defined by 10 CFR 50.36 is the same as the OPERABILITY limit for these devices. However, use of the trip setpoint to define OPERABILITY in Technical Specifications and its corresponding designation as the LSSS required by 10 CFR 50.36 would be an overly restrictive requirement if it were applied as an OPERABILITY limit for the "as found" value of a protective device setting during a Surveillance. This would result in Technical Specification compliance problems, as well as reports and corrective actions required by the rule which are not necessary to ensure safety. For example, an automatic protective device with a setting that has been found to be different from the trip setpoint due to some drift of the setting may still be OPERABLE since drift is to be expected. This expected drift would have been specifically accounted for in the setpoint methodology for calculating the trip setpoint and thus the automatic protective action would still have ensured that the SL would not be exceeded with the "as found" setting of the protective device. Therefore, the device would still be OPERABLE since it would have performed its safety function and the only corrective action required would be to reset the device to the trip setpoint to account for further drift during the next surveillance interval.

Use of the trip setpoint to define "as found" OPERABILITY and its designation as the LSSS under the expected circumstances described above would result in actions required by both the rule and Technical Specifications that are clearly not warranted. However, there is also some point beyond which the device would have not been able to perform its function due, for example, to greater than expected drift. This value needs to be specified in the Technical Specifications in order to define OPERABILITY of the devices and is designated as the Allowable Value which, as stated above, is the same as the LSSS.

The Allowable Valuable specified in Table 3.3.1-1 serves as the LSSS such that a channel is OPERABLE if the trip setpoint is found not to exceed the Allowable Value during the CHANNEL FUNCTIONAL TEST (CFT). As such, the Allowable Value differs from the trip setpoint by an amount primarily equal to the expected instrument loop uncertainties, such as drift, during the surveillance interval. In this manner, the actual setting of the device will still meet the LSSS definition and ensure that a SL is not exceeded at any given point of time as long as the device has

BASES

BACKGROUND (continued)

not drifted beyond that expected during the surveillance interval. If the actual setting of the device is found to have exceeded the Allowable Value the device would be considered inoperable from a Technical Specification perspective. This requires corrective action including those actions required by 10 CFR 50.36 when automatic protective devices do not function as required. Note that, although the channel is "OPERABLE" under these circumstances, the trip setpoint should be left adjusted to a value within the established trip setpoint calibration tolerance band, in accordance with uncertainty assumptions stated in the referenced setpoint methodology (as-left criteria), and confirmed to be operating within the statistical allowances of the uncertainty terms assigned.

During AOOs, which are those events expected to occur one or more times during the plant life, the acceptable limits are:

- The departure from nucleate boiling ratio (DNBR) shall be maintained above the Safety Limit (SL) value to prevent departure from nucleate boiling,
- Fuel centerline melting shall not occur, and
- The Reactor Coolant System (RCS) pressure SL of 2750 psia shall not be exceeded.

Maintaining the parameters within the above values ensures that the offsite dose will be within the 10 CFR 50 (Ref. 2) and 10 CFR 100 (Ref. 3) criteria during AOOs.

Accidents are events that are analyzed even though they are not expected to occur during the plant life. The acceptable limit during accidents is that the offsite dose shall be maintained within an acceptable fraction of 10 CFR 100 (Ref. 3) limits. Different accident categories allow a different fraction of these limits based on probability of occurrence. Meeting the acceptable dose limit for an accident category is considered having acceptable consequences for that event.

The RPS is segmented into four interconnected modules. These modules are:

- Measurement channels,

BASES

BACKGROUND (continued)

- Bistable trip units,
- RPS Logic, and
- Reactor trip circuit breakers (RTCBs).

This LCO addresses measurement channels and bistable trip units. It also addresses the automatic bypass removal feature for those trips with operating bypasses. The RPS Logic and RTCBs are addressed in LCO 3.3.3, "Reactor Protective System (RPS) Logic and Trip Initiation."

The role of each of these modules in the RPS, including those associated with the logic and RTCBs, is discussed below.

Measurement Channels

Measurement channels, consisting of field transmitters or process sensors and associated instrumentation, provide a measurable electronic signal based upon the physical characteristics of the parameter being measured.

The excore nuclear instrumentation and the analog core protection calculators (CPCs) are considered components in the measurement channels. The wide range nuclear instruments (NIs) provide a Power Rate of Change - High Trip. Three RPS trips use a power level designated as Q power as an input. Q power is the higher of NI power and primary calorimetric power (ΔT power) based on RCS hot leg and cold leg temperatures. Trips using Q power as an input include the Variable High Power Trip (VHPT) - High, Thermal Margin/Low Pressure (TM/LP), and the Axial Power Distribution (APD) - High trips.

The analog CPCs provide the complex signal processing necessary to calculate the TM/LP trip setpoint, APD trip setpoint, VHPT trip setpoint, and Q power calculation.

The excore NIs (wide range and power range) and the analog CPCs (TM/LP and APD calculators) are mounted in the RPS cabinet, with one channel of each in each of the four RPS bays.

BASES

BACKGROUND (continued)

Four identical measurement channels with electrical and physical separation are provided for each parameter used in the direct generation of trip signals. These are designated channels A through D. Measurement channels provide input to one or more RPS bistables within the same RPS channel. In addition, some measurement channels may also be used as inputs to Engineered Safety Features Actuation System (ESFAS) bistables, and most provide indication in the control room. Measurement channels used as an input to the RPS are never used for control functions.

When a channel monitoring a parameter exceeds a predetermined setpoint, indicating an unsafe condition, the bistable monitoring the parameter in that channel will trip. Tripping two or more channels of bistables monitoring the same parameter de-energizes Matrix Logic, which in turn de-energizes the Initiation Logic. This causes all eight RTCBs to open, interrupting power to the control element assemblies (CEAs), allowing them to fall into the core.

Three of the four measurement and bistable channels are necessary to meet the redundancy and testability of GDC 21 in 10 CFR 50, Appendix A (Ref. 2). The fourth channel provides additional flexibility by allowing one channel to be removed from service (trip channel bypass) for maintenance or testing while still maintaining a minimum two-out-of-three logic. Thus, even with a channel inoperable, no single additional failure in the RPS can either cause an inadvertent trip or prevent a required trip from occurring.

Since no single failure will either cause or prevent a protective system actuation, and no protective channel feeds a control channel, this arrangement meets the requirements of IEEE Standard 279-1971 (Ref. 4).

Many of the RPS trips are generated by comparing a single measurement to a fixed bistable setpoint. Certain Functions, however, make use of more than one measurement to provide a trip. The following trips use multiple measurement channel inputs:

- <u>Steam Generator Level - Low</u>

  This trip uses the lower of the two steam generator levels as an input to a common bistable.

BASES

BACKGROUND (continued)

- Steam Generator Pressure - Low

  This trip uses the lower of the two steam generator pressures as an input to a common bistable.

- Variable High Power Trip (VHPT) - High

  The VHPT uses Q power as its only input. Q power is the higher of NI power and ΔT power. It has a trip setpoint that tracks power levels downward so that it is always within a fixed increment above current power, subject to a minimum value.

  On power increases, the trip setpoint remains fixed unless manually reset, at which point it increases to the new setpoint, a fixed increment above Q power at the time of reset, subject to a maximum value. Thus, during power escalation, the trip setpoint must be repeatedly reset to avoid a reactor trip.

- Thermal Margin/Low Pressure (TM/LP) and Steam Generator Pressure Difference

  Q power is only one of several inputs to the TM/LP trip. Other inputs include internal ASI and cold leg temperature based on the higher of two cold leg resistance temperature detectors. The TM/LP trip setpoint is a complex function of these inputs and represents a minimum acceptable RCS pressure to be compared to actual RCS pressure in the TM/LP trip unit.

  Steam generator pressure is also an indirect input to the TM/LP trip via the Steam Generator Pressure Difference. This Function provides a reactor trip when the secondary pressure in either steam generator exceeds that of the other generator by greater than a fixed amount. The trip is implemented by biasing the TM/LP trip setpoint upward so as to ensure TM/LP trip if an asymmetric steam generator transient is detected.

- Axial Power Distribution (APD) - High

  Q Power and ASI are inputs to the APD trip. The APD trip setpoint is a function of Q power, being more restrictive at higher power levels. It provides a reactor trip if actual ASI exceeds the APD trip setpoint.

BASES

BACKGROUND (continued)

Bistable Trip Units

Bistable trip units, mounted in the RPS cabinet, receive an analog input from the measurement channels, compare the analog input to trip setpoints, and provide contact output to the Matrix Logic. They also provide local trip indication and remote annunciation.

There are four channels of bistable trip units, designated A through D, for each RPS Function, one for each measurement channel. Bistable output relays de-energize when a trip occurs.

The contacts from these bistable relays are arranged into six coincidence matrices, comprising the Matrix Logic. If bistables monitoring the same parameter in at least two channels trip, the Matrix Logic will generate a reactor trip (two-out-of-four logic).

Some of the RPS measurement channels provide contact outputs to the RPS, so the comparison of an analog input to a trip setpoint is not necessary. In these cases, the bistable trip unit is replaced with an auxiliary trip unit. The auxiliary trip units provide contact multiplication so the single input contact opening can provide multiple contact outputs to the coincidence logic as well as trip indication and annunciation.

Trips employing auxiliary trip units include the Loss of Load trip and the APD - High trip. The Loss of Load trip is a contact input from the Electro Hydraulic Control System control oil pressure on each of the four high pressure stop valves.

The APD trip, described above, is a complex function in which the actual trip comparison is performed within the CPC. Therefore the APD - High trip unit employs a contact input from the CPC.

All RPS trips, with the exception of the Loss of Load trip, generate a pretrip alarm as the trip setpoint is approached.

The trip setpoints used in the bistable trip units are based on the analytical limits stated in Reference 5. The selection of these trip setpoints is such that adequate protection is provided when all sensor and processing time delays are taken into account. To allow for calibration tolerances, instrumentation uncertainties, instrument drift, and severe environment errors - for those RPS channels that must function in harsh environments, as defined by 10 CFR 50.49 (Ref. 6) - Allowable Values specified in Table 3.3.1-1, in the accompanying LCO, are

BASES

BACKGROUND (continued)

conservatively adjusted with respect to the analytical limits. A detailed description of the methodology used to calculate the trip setpoints, including their explicit uncertainties, is provided in the "Plant Protection System Selection of Trip Setpoint Values" (Ref. 7). The nominal trip setpoint entered into the bistable is normally still more conservative than that specified by the Allowable Value, to account for changes in random measurement errors detectable by a CHANNEL FUNCTIONAL TEST. One example of such a change in measurement error is drift during the interval between surveillances. A channel is inoperable if its actual setpoint is not within its required Allowable Value.

Setpoints in accordance with the Allowable Value will ensure that SLs of Chapter 2.0 are not violated during AOOs and the consequences of DBAs will be acceptable, providing the plant is operated from within the LCOs at the onset of the AOO or DBA and the equipment functions as designed.

Note that in the accompanying LCO 3.3.1, the Allowable Values of Table 3.3.1-1 are the LSSS.

RPS Logic

The RPS Logic, addressed in LCO 3.3.3, consists of both Matrix and Initiation Logic and employs a scheme that provides a reactor trip when bistables in any two out of the four channels sense the same input parameter trip. This is called a two-out-of-four trip logic. This logic and the RTCB configuration are shown in Figure B 3.3.1-1.

Bistable relay contact outputs from the four channels are configured into six logic matrices. Each logic matrix checks for a coincident trip in the same parameter in two bistable channels. The matrices are designated the AB, AC, AD, BC, BD, and CD matrices to reflect the bistable channels being monitored. Each logic matrix contains four normally energized matrix relays. When a coincidence is detected, consisting of a trip in the same Function in the two channels being monitored by the logic matrix, all four matrix relays de-energize.

The matrix relay contacts are arranged into trip paths, with one of the four matrix relays in each matrix opening contacts in one of the four trip paths. Each trip path provides power to one of the four normally energized RTCB control relays (K1, K2, K3, and K4). The trip paths thus each have six contacts in series, one from each matrix, and perform a logical OR function, opening the RTCBs if any one or more of the six logic matrices indicate a coincidence condition.

BASES

BACKGROUND (continued)

Each trip path is responsible for opening one set of two of the eight RTCBs. The RTCB control relays (K-relays), when de-energized, interrupt power to the breaker undervoltage trip attachments and simultaneously apply power to the shunt trip attachments on each of the two breakers. Actuation of either the undervoltage or shunt trip attachment is sufficient to open the RTCB and interrupt power from the motor generator (MG) sets to the control element drive mechanisms (CEDMs).

When a coincidence occurs in two RPS channels, all four matrix relays in the affected matrix de-energize. This in turn de-energizes all four RTCB control relays, which simultaneously de-energize the undervoltage and energize the shunt trip attachments in all eight RTCBs, tripping them open.

Matrix Logic refers to the matrix power supplies, trip channel bypass contacts, and interconnecting matrix wiring between bistable and auxiliary trip units, up to but not including the matrix relays. Contacts in the bistable and auxiliary trip units are excluded from the Matrix Logic definition, since they are addressed as part of the measurement channel.

The Initiation Logic consists of the trip path power source, matrix relays and their associated contacts, all interconnecting wiring, and solid state (auxiliary) relays through the K-relay contacts in the RTCB control circuitry.

It is possible to change the two-out-of-four RPS Logic to a two-out-of-three logic for a given input parameter in one channel at a time by trip channel bypassing select portions of the Matrix Logic. Trip channel bypassing a bistable effectively shorts the bistable relay contacts in the three matrices associated with that channel. Thus, the bistables will function normally, producing normal trip indication and annunciation, but a reactor trip will not occur unless two additional channels indicate a trip condition. Trip channel bypassing can be simultaneously performed on any number of parameters in any number of channels, providing each parameter is bypassed in only one channel at a time. An interlock prevents simultaneous trip channel bypassing of the same parameter in more than one channel. Trip channel bypassing is normally employed during maintenance or testing.

BASES

BACKGROUND (continued)

For those plants that have demonstrated sufficient channel to channel independence, two-out-of-three logic is the minimum that is required to provide adequate plant protection, since a failure of one channel still ensures a reactor trip would be generated by the two remaining OPERABLE channels. Two-out-of-three logic also prevents inadvertent trips caused by any single channel failure in a trip condition.

In addition to the trip channel bypasses, there are also operating bypasses on select RPS trips. Some of these bypasses are enabled manually, others automatically, in all four RPS channels when plant conditions do not warrant the specific trip protection. All operating bypasses are automatically removed when enabling bypass conditions are no longer satisfied. Trips with operating bypasses include Power Rate of Change - High, Reactor Coolant Flow - Low, Steam Generator Pressure - Low, APD - High, TM/LP, and Steam Generator Pressure Difference. [The Loss of Load trip, Power Rate of Change - High, and APD - High operating bypasses are automatically enabled and disabled.]

<u>Reactor Trip Circuit Breakers (RTCBs)</u>

The reactor trip switchgear, addressed in LCO 3.3.3 and shown in Figure B 3.3.1-1, consists of eight RTCBs, which are operated in four sets of two breakers (four channels). Power input to the reactor trip switchgear comes from two full capacity MG sets operated in parallel such that the loss of either MG set does not de-energize the CEDMs. There are two separate CEDM power supply buses, each bus powering half of the CEDMs. Power is supplied from the MG sets to each bus via two redundant paths (trip legs). Trip legs 1A and 1B supply power to CEDM bus 1. Trip legs 2A and 2B supply power to CEDM bus 2. This ensures that a fault or the opening of a breaker in one trip leg (i.e., for testing purposes) will not interrupt power to the CEDM buses.

Each of the four trip legs consists of two RTCBs in series. The two RTCBs within a trip leg are actuated by separate initiation circuits.

The eight RTCBs are operated as four sets of two breakers (four channels). For example, if a breaker receives an open signal in trip leg A (for CEDM bus 1), an identical breaker in trip leg B (for CEDM bus 2) will also receive an open signal. This arrangement ensures that power is interrupted to both CEDM buses, thus preventing trip of only half of the CEAs (a half trip). Any one inoperable breaker in a channel will make the entire channel inoperable.

BASES

BACKGROUND (continued)

Each set of RTCBs is operated by either a Manual Trip push button or an RPS actuated K-relay. There are four Manual Trip push buttons, arranged in two sets of two, as shown in Figure B 3.3.1-1. Depressing both push buttons in either set will result in a reactor trip.

When a Manual Trip is initiated using the control room push buttons, the RPS trip paths and K-relays are bypassed, and the RTCB undervoltage and shunt trip attachments are actuated independent of the RPS.

Manual Trip circuitry includes the push button and interconnecting wiring to both RTCBs necessary to actuate both the undervoltage and shunt trip attachments but excludes the K-relay contacts and their interconnecting wiring to the RTCBs, which are considered part of the Initiation Logic.

Functional testing of the entire RPS, from bistable input through the opening of individual sets of RTCBs, can be performed either at power or shutdown and is normally performed on a quarterly basis.
FSAR, Section [7.2] (Ref. 8), explains RPS testing in more detail.

APPLICABLE SAFETY ANALYSES

Each of the analyzed accidents and transients can be detected by one or more RPS Functions. The accident analysis contained in Reference 5 takes credit for most RPS trip Functions. Functions not specifically credited in the accident analysis are part of the NRC approved licensing basis for the plant. These Functions may provide protection for conditions that do not require dynamic transient analysis to demonstrate Function performance. Other Functions, such as the Loss of Load trip, are purely equipment protective, and their use minimizes the potential for equipment damage.

The specific safety analyses applicable to each protective Function are identified below:

1. Variable High Power Trip (VHPT) - High

   The VHPT provides reactor core protection against positive reactivity excursions that are too rapid for a Pressurizer Pressure - High or TM/LP trip to protect against. The following events require VHPT protection:

   - Uncontrolled CEA withdrawal event,
   - Excess load,

BASES

APPLICABLE SAFETY ANALYSES (continued)

- Excess feedwater heat removal event,
- CEA ejection event, and
- Main steam line break (MSLB) (outside containment).

The first three events are AOOs, and fuel integrity is maintained. The fourth and fifth are accidents, and limited fuel damage may occur.

2. Power Rate of Change - High

The Power Rate of Change - High trip is used to trip the reactor when excore [logarithmic] power indicates an excessive rate of change. The Power Rate of Change - High Function minimizes transients for events such as a continuous CEA withdrawal or a boron dilution event from low power levels. The trip may be bypassed when THERMAL POWER is < 1E-4% RTP, when poor counting statistics may lead to erroneous indication. It is also bypassed at > 15% RTP, where moderator temperature coefficient and fuel temperature coefficient make high rate of change of power unlikely. With the RTCBs open, the Power Rate of Change - High trip is not required to be OPERABLE; however, the indication and alarm Functions of at least two channels are required by LCO 3.3.13, "[Logarithmic] Power Monitoring Channels," to be OPERABLE. LCO 3.3.13 ensures the [logarithmic] channels are available to detect and alert the operator to a boron dilution event.

3. Reactor Coolant Flow - Low

The Reactor Coolant Flow - Low trip provides protection during the following events:

- Loss of RCS flow,
- Loss of nonemergency AC power,
- Reactor coolant pump (RCP) seized shaft,
- RCP sheared shaft, and
- Certain MSLB events.

The loss of RCS flow and of nonemergency AC power events are AOOs where fuel integrity is maintained. The RCP seized shaft, sheared shaft, and MSLBs are accidents where fuel damage may result.

BASES

APPLICABLE SAFETY ANALYSES (continued)

4. Pressurizer Pressure - High

The Pressurizer Pressure - High trip, in conjunction with pressurizer safety valves and main steam safety valves (MSSVs), provides protection against overpressure conditions in the RCS during the following events:

- Loss of condenser vacuum with a concurrent loss of offsite power,
- Loss of condenser vacuum with a concurrent loss of one 6.9 kV bus,
- Isolation of turbine at 102% power,
- Feedwater System pipe breaks between the steam generator and check valve,
- CEA withdrawal, and
- Loss of feedwater flow.

5. Containment Pressure - High

The Containment Pressure - High trip prevents exceeding the containment design pressure during certain loss of coolant accidents (LOCAs) or feedwater line break accidents. It ensures a reactor trip prior to, or concurrent with, a LOCA, thus assisting the ESFAS in the event of a LOCA or MSLB. Since these are accidents, SLs may be violated. However, the consequences of the accident will be acceptable.

6. Steam Generator Pressure - Low

The Steam Generator Pressure - Low trip provides protection against an excessive rate of heat extraction from the steam generators, which would result in a rapid uncontrolled cooldown of the RCS. This trip is needed to shut down the reactor and assist the ESFAS in the event of an MSLB. Since these are accidents, SLs may be violated. However, the consequences of the accident will be acceptable.

BASES

APPLICABLE SAFETY ANALYSES (continued)

7.a, 7.b. Steam Generator A and B Level - Low

The Steam Generator A Level - Low and Steam Generator B Level - Low trips are required for the following events:

- Steam System piping failures,
- Feedwater System pipe breaks,
- Inadvertent opening of a steam generator atmospheric dump valve (ADV),
- Loss of normal feedwater, and
- Asymmetric loss of feedwater.

The Steam Generator Level - Low trip ensures that low DNBR, high local power density, and the RCS pressure SLs are maintained during normal operation and AOOs, and, in conjunction with the ESFAS, the consequences of the Feedwater System pipe break accident will be acceptable.

8. Axial Power Distribution (APD) - High

The APD - High trip ensures that excessive axial peaking, such as that due to axial xenon oscillations, will not cause fuel damage. It ensures that neither a DNBR less than the SL nor a peak linear heat rate that corresponds to the temperature for fuel centerline melting will occur. This trip is the primary protection against fuel centerline melting.

9. Thermal Margin

a. Thermal Margin/Low Pressure (TM/LP)

The TM/LP trip prevents exceeding the DNBR SL during AOOs and aids the ESFAS during certain accidents. The following events require TM/LP protection:

BASES

APPLICABLE SAFETY ANALYSES (continued)

- Excess load (inadvertent opening of a steam generator ADV),
- RCS depressurization (inadvertent safety or power operated relief valves (PORVs) opening),
- Steam generator tube rupture, and
- LOCA accident.

The first two events are AOOs, and fuel integrity is maintained. The third and fourth are accidents, and limited fuel damage may occur although only the LOCA is expected to result in fuel damage. The trip is initiated whenever the RCS pressure signal drops below a minimum value (P_{min}) or a computed value (P_{var}) as described below, whichever is higher. The computed value is a Function Q power, ASI, as determined from the axially split excore detectors, reactor inlet (cold leg) temperature, and the number of RCPs operating.

The minimum value of reactor coolant flow rate, the maximum T_Q, and the maximum CEA deviation permitted for continuous operation are assumed in the generation of this trip Function. In addition, CEA group sequencing in accordance with LCO 3.1.6, "Regulating Control Element Assembly (CEA) Insertion Limits," is assumed. Finally, the maximum insertion of CEA banks that can occur during any AOO prior to a VHPT is assumed.

b. Steam Generator Pressure Difference

The Steam Generator Pressure Difference provides protection for those AOOs associated with secondary system malfunctions that result in asymmetric primary coolant temperatures. The most limiting event is closure of a single main steam isolation valve. Steam Generator Pressure Difference is provided by comparing the secondary pressure in both steam generators in the TM/LP calculator. If the pressure in either exceeds that in the other by the trip setpoint, a TM/LP trip will result.

BASES

APPLICABLE SAFETY ANALYSES (continued)

10. Loss of Load

The Loss of Load (turbine stop valve (TSV) control oil pressure) trip is anticipatory for the loss of heat removal capabilities of the secondary system following a turbine trip. The Loss of Load trip prevents lifting the pressurizer safety valves, PORVs, and MSSVs in the event of a turbine generator trip. Thus, the trip minimizes the pressure and temperature transients on the reactor by initiating a trip well before reaching the Pressurizer Pressure - High trip and pressurizer safety valve setpoints. The four RPS Loss of Load reactor trip channels receive their input from sensors mounted on the high pressure TSV actuators. Since there are four high pressure TSVs, one actuator per valve and one sensor per actuator, each sensor sends its signal to a different RPS channel. When the turbine trips, control oil is dumped from the high pressure TSVs. When the control oil pressure drops to the appropriate setpoint, a reactor trip signal is generated.

Interlocks/Bypasses

The bypasses and their Allowable Values are addressed in footnotes to Table 3.3.1-1. They are not otherwise addressed as specific Table entries.

The automatic bypass removal features must function as a backup to manual actions for all safety related trips to ensure the trip Functions are not operationally bypassed when the safety analysis assumes the Functions are not bypassed. The RPS operating bypasses are:

Zero power mode bypass (ZPMB) removal on the TM/LP, Steam Generator Pressure Difference, and reactor coolant low flow trips when THERMAL POWER is < 1E-4% RTP. This bypass is manually enabled below the specified setpoint to permit low power testing. The wide range NI Level 1 bistable in the wide range drawer permits manual bypassing below the setpoint and removes the bypass above the setpoint.

Power rate of change bypass removal. The Power Rate of Change - High trip is automatically bypassed at < 1E-4% RTP, as sensed by the wide range NI Level 2 bistable, and at > 12% RTP by the power range NI Level 1 bistable, mounted in their respective NI drawers. Automatic bypass removal is also effected by these bistables when conditions are no longer satisfied.

BASES

APPLICABLE SAFETY ANALYSES (continued)

Loss of Load and APD - High bypass removal. The Loss of Load and APD - High trips are automatically bypassed when at < 15% RTP as sensed by the power range NI Level 1 bistable. The bypass is automatically removed by this bistable above the setpoint. This same bistable is used to bypass the Power Rate of Change - High trip.

Steam Generator Pressure - Low bypass removal. The Steam Generator Pressure - Low trip is manually enabled below the pretrip setpoint. The permissive is removed, and the bypass automatically removed, when the Steam Generator Pressure - Low pretrip clears.

The RPS instrumentation satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

The LCO requires all instrumentation performing an RPS Function to be OPERABLE. Failure of any required portion of the instrument channel renders the affected channel(s) inoperable and reduces the reliability of the affected Functions. The specific criteria for determining channel OPERABILITY differ slightly between Functions. These criteria are discussed on a Function by Function basis below.

Actions allow maintenance (trip channel) bypass of individual channels, but the bypass activates interlocks that prevent operation with a second channel in the same Function bypassed. Plants are restricted to 48 hours in a trip channel bypass condition before either restoring the Function to four channel operation (two-out-of-four logic) or placing the channel in trip (one-out-of-three logic). At plants where adequate channel to channel independence has been demonstrated, specific exceptions may be approved by the NRC staff to permit one of the two-out-of-four channels to be bypassed for an extended period of time.

Only the Allowable Values are specified for each RPS trip Function in the LCO. Nominal trip setpoints are specified in the plant specific setpoint calculations. The nominal setpoints are selected to ensure the setpoints measured by CHANNEL FUNCTIONAL TESTS do not exceed the Allowable Value if the bistable is performing as required. Operation with a trip setpoint less conservative than the nominal trip setpoint, but within its Allowable Value, is acceptable, provided that operation and testing are consistent with the assumptions of the plant specific setpoint calculations. Each Allowable Value specified is more conservative than the analytical limit assumed in the safety analysis in order to account for instrument uncertainties appropriate to the trip Function. These uncertainties are defined in the "Plant Protection System Selection of Trip Setpoint Values" (Ref. 7).

BASES

LCO (continued)

The following Bases for each trip Function identify the above RPS trip Function criteria items that are applicable to establish the trip Function OPERABILITY.

1. Variable High Power Trip (VHPT) - High

   This LCO requires all four channels of the VHPT to be OPERABLE in MODES 1 and 2.

   The Allowable Value is high enough to provide an operating envelope that prevents unnecessary Linear Power Level - High reactor VHPT - High trips during normal plant operations. The Allowable Value is low enough for the system to maintain a margin to unacceptable fuel cladding damage should a CEA ejection accident occur.

   The VHPT setpoint is operator adjustable and can be set at a fixed increment above the indicated THERMAL POWER level. Operator action is required to increase the trip setpoint as THERMAL POWER is increased. The trip setpoint is automatically decreased as THERMAL POWER decreases. The trip setpoint has a maximum and a minimum setpoint.

   Adding to this maximum value the possible variation in trip setpoint due to calibration and instrument errors, the maximum actual steady state THERMAL POWER level at which a trip would be actuated is 112% RTP, which is the value used in the safety analyses.

   To account for these errors, the safety analysis minimum value is 40% RTP. The 10% step is a maximum value assumed in the safety analysis. There is no uncertainty applied to the step.

2. Power Rate of Change - High

   This LCO requires four channels of Power Rate of Change - High to be OPERABLE in MODES 1 and 2, as well as in MODES 3, 4, and 5 when the RTCBs are closed and the CEA Drive System is capable of CEA withdrawal.

   The high power rate of change trip serves as a backup to the administratively enforced startup rate limit. The Function is not credited in the accident analyses; therefore, the Allowable Value for the trip or bypass Functions is not derived from analytical limits.

BASES

LCO (continued)

3. Reactor Coolant Flow - Low

This LCO requires four channels of Reactor Coolant Flow - Low to be OPERABLE in MODES 1 and 2.

The trip may be manually bypassed when THERMAL POWER falls below 1E-4% RTP. This bypass is part of the ZPMB circuitry, which also bypasses the TM/LP trip and provides a ΔT power block signal to the Q power select logic. This ZPMB allows low power physics testing at reduced RCS temperatures and pressures. It also allows heatup and cooldown with shutdown CEAs withdrawn.

This trip is set high enough to maintain fuel integrity during a loss of flow condition. The setting is low enough to allow for normal operating fluctuations from offsite power. To account for analysis uncertainty, the value in the safety analysis is 93% RTP.

4. Pressurizer Pressure - High

This LCO requires four channels of Pressurizer Pressure - High to be OPERABLE in MODES 1 and 2.

The Allowable Value is set high enough to allow for pressure increases in the RCS during normal operation (i.e., plant transients) not indicative of an abnormal condition. The setting is below the lift setpoint of the pressurizer safety valves and low enough to initiate a reactor trip when an abnormal condition is indicated. The difference between the Allowable Value and the analysis setpoint of 2470 psia includes allowance for harsh environment.

The Pressurizer Pressure - High trip concurrent with PORV operation avoids unnecessary operation of the pressurizer safety valves.

5. Containment Pressure - High

This LCO requires four channels of Containment Pressure - High to be OPERABLE in MODES 1 and 2.

The Allowable Value is high enough to allow for small pressure increases in containment expected during normal operation (i.e., plant heatup) that are not indicative of an abnormal condition. The setting is low enough to initiate a reactor trip to prevent containment pressure from exceeding design pressure following a DBA.

BASES

LCO (continued)

6. Steam Generator Pressure - Low

This LCO requires four channels of Steam Generator Pressure - Low per steam generator to be OPERABLE in MODES 1 and 2.

The Allowable Value is sufficiently below the full load operating value for steam pressure so as not to interfere with normal plant operation, but still high enough to provide the required protection in the event of excessive steam demand. Since excessive steam demand causes the RCS to cool down, resulting in positive reactivity addition to the core, a reactor trip is required to offset that effect.

The difference between the Allowable Value and the safety analysis value of 600 psia includes harsh environment uncertainties.

The Function may be manually bypassed as steam generator pressure is reduced during controlled plant shutdowns. This bypass is permitted at a preset steam generator pressure. The bypass, in conjunction with the ZPMB, allows testing at low temperatures and pressures, and heatup and cooldown with the shutdown CEAs withdrawn. From a bypass condition the trip will be reinstated automatically as steam generator pressure increases above the preset pressure.

7.a, 7.b. Steam Generator Level – Low

This LCO requires four channels of Steam Generator Level - Low per steam generator to be OPERABLE in MODES 1 and 2.

The Allowable Value is sufficiently below the normal operating level for the steam generators so as not to cause a reactor trip during normal plant operations. The trip setpoint is high enough to ensure a reactor trip signal is generated before water level drops below the top of the feed ring. The difference between the Allowable Value and the measurement value includes 10 inches of measurement uncertainty. The specified setpoint ensures there will be sufficient water inventory to provide a 10 minute margin before auxiliary feedwater is required for the removal of decay heat.

BASES

LCO (continued)

8. Axial Power Distribution (APD) - High

This LCO requires four channels of APD - High to be OPERABLE in MODE 1 ≥ 15% RTP.

The Allowable Value curve was derived from an analysis of many axial power shapes with allowances for instrumentation inaccuracies and the uncertainty associated with the excore to incore ASI relationship.

The APD trip is automatically bypassed at < 15% RTP, where it is not required for reactor protection.

9. Thermal Margin

a. Thermal Margin/Low Pressure (TM/LP)

This LCO requires four channels of TM/LP to be OPERABLE in MODES 1 and 2.

The Allowable Value includes allowances for equipment response time, measurement uncertainties, processing error, and a further allowance to compensate for the time delay associated with providing effective termination of the occurrence that exhibits the most rapid decrease in margin to the SL.

This trip may be manually bypassed when THERMAL POWER falls below 1E-4% RTP. This bypass is part of the ZPMB circuitry, which also bypasses the Reactor Coolant Flow - Low trip and provides a ΔT power block signal to the Q power select logic. This ZPMB allows low power physics testing at reduced RCS temperatures and pressures. It also allows heatup and cooldown with shutdown CEAs withdrawn.

b. Steam Generator Pressure Difference

This LCO requires four channels of Steam Generator Pressure Difference to be OPERABLE in MODES 1 and 2.

BASES

LCO (continued)

The Allowable Value is high enough to avoid trips caused by normal operation and minor transients, but ensures DNBR protection in the event of Design Basis Events. The difference between the Allowable Value and the 175 psia analysis setpoint allows for 40 psia of measurement uncertainty.

The trip may be bypassed when THERMAL POWER falls below 1E-4% RTP. The Steam Generator Pressure Difference is subject to the ZPMB, since it is an input to the TM/LP trip and is not required for protection at low power levels.

10. Loss of Load

The LCO requires four Loss of Load trip channels to be OPERABLE in MODE 1 $\geq$ 15% RTP.

The Loss of Load trip may be bypassed when THERMAL POWER falls below 15%, since it is no longer needed to prevent lifting of the pressurizer safety valves, steam generator safety valves, or PORVs in the event of a Loss of Load. The Nuclear Steam Supply System and the Steam Dump System are capable of accommodating the Loss of Load without requiring the use of the above equipment.

Interlocks/Bypasses

The LCO on bypass permissive removal channels requires that the automatic bypass removal feature of all four operating bypass channels be OPERABLE for each RPS Function with an operating bypass in the MODES addressed in the specific LCO for each Function. All four bypass removal channels must be OPERABLE to ensure that none of the four RPS channels are inadvertently bypassed.

The LCO applies to the bypass removal feature only. If the bypass enable Function is failed so as to prevent entering a bypass condition, operation may continue.

The interlock Allowable Values are based on analysis requirements for the bypassed functions. These are discussed above as part of the LCO discussion for the affected Functions.

BASES

APPLICABILITY

This LCO is applicable in accordance with Table 3.3.1-1. Most RPS trips are required to be OPERABLE in MODES 1 and 2 because the reactor is critical in these MODES. The trips are designed to take the reactor subcritical, maintaining the SLs during AOOs and assisting the ESFAS in providing acceptable consequences during accidents. Exceptions are addressed in footnotes to the table. Exceptions to this APPLICABILITY are:

- The APD - High Trip and Loss of Load are only applicable in MODE 1 ≥ 15% RTP because they may be automatically bypassed at < 15% RTP, where they are no longer needed.

- The Power Rate of Change - High trip, RPS Logic, RTCBs, and Manual Trip are also required in MODES 3, 4, and 5, with the RTCBs closed, to provide protection for boron dilution and CEA withdrawal events. The Power Rate of Change - High trip in these lower MODES is addressed in LCO 3.3.2, "Reactor Protective System (RPS) Instrumentation - Shutdown." The RPS Logic in MODES 1, 2, 3, 4, and 5 is addressed in LCO 3.3.3.

Most trips are not required to be OPERABLE in MODES 3, 4, and 5. In MODES 3, 4, and 5, the emphasis is placed on return to power events. The reactor is protected in these MODES by ensuring adequate SDM.

ACTIONS

The most common causes of channel inoperability are outright failure or drift of the bistable or process module sufficient to exceed the tolerance allowed by the plant specific setpoint analysis. Typically, the drift is found to be small and results in a delay of actuation rather than a total loss of function. This determination is generally made during the performance of a CHANNEL FUNCTIONAL TEST when the process instrument is set up for adjustment to bring it to within specification. If the trip setpoint is less conservative than the Allowable Value in Table 3.3.1-1, the channel is declared inoperable immediately, and the appropriate Condition(s) must be entered immediately.

In the event a channel's trip setpoint is found nonconservative with respect to the Allowable Value, or the transmitter, instrument loop, signal processing electronics, or RPS bistable trip unit is found inoperable, then all affected Functions provided by that channel must be declared inoperable, and the plant must enter the Condition for the particular protection Function affected.

When the number of inoperable channels in a trip Function exceeds that specified in any related Condition associated with the same trip Function, then the plant is outside the safety analysis. Therefore, LCO 3.0.3 is immediately entered if applicable in the current MODE of operation.

BASES

ACTIONS (continued)

A Note has been added to the ACTIONS to clarify the application of the Completion Time rules. The Conditions of this Specification may be entered independently for each Function. The Completion Times of each inoperable Function will be tracked separately for each Function, starting from the time the Condition was entered.

A.1, A.2.1, and A.2.2

Condition A applies to the failure of a single channel in any RPS automatic trip Function. RPS coincidence logic is normally two-out-of-four.

If one RPS bistable trip unit or associated instrument channel is inoperable, startup or power operation is allowed to continue, providing the inoperable trip unit is placed in bypass or trip within 1 hour (Required Action A.1). With one channel in bypass, no additional random failure of a single channel could spuriously trip the reactor and a valid trip signal can still trip the reactor. With one channel in trip, an additional random failure of a single channel could spuriously trip the reactor. Therefore, it is preferable to place an inoperable channel in bypass rather than trip.

The Completion Time of 1 hour allotted to restore, bypass, or trip the channel is sufficient to allow the operator to take all appropriate actions for the failed channel while ensuring that the risk involved in operating with the failed channel is acceptable.

The failed channel is restored to OPERABLE status or is placed in trip within [48] hours (Required Action A.2.1 or Required Action A.2.2). Required Action A.2.1 restores the full capability of the Function.

[Required Action A.2.2 places the Function in a one-out-of-three configuration. In this configuration, common cause failure of dependent channels cannot prevent trip.]

The Completion Time of [48] hours is based on operating experience, which has demonstrated that a random failure of a second channel occurring during the [48] hour period is a low probability event.

BASES

ACTIONS (continued)

B.1 and B.2

Condition B applies to the failure of two channels in any RPS automatic trip Function.

Required Action B.1 provides for placing one inoperable channel in bypass and the other channel in trip within the Completion Time of 1 hour. This Completion Time is sufficient to allow the operator to take all appropriate actions for the failed channels while ensuring that the risk involved in operating with the failed channels is acceptable. With one channel of protective instrumentation bypassed, the RPS is in a two-out-of-three logic; but with another channel failed, the RPS may be operating in a two-out-of-two logic. This is outside the assumptions made in the analyses and should be corrected. To correct the problem, the second channel is placed in trip. This places the RPS in a one-out-of-two logic. If any of the other OPERABLE channels receives a trip signal, the reactor will trip.

One channel should be restored to OPERABLE status within [48] hours for reasons similar to those stated under Condition A. After one channel is restored to OPERABLE status, the provisions of Condition A still apply to the remaining inoperable channel. Therefore, the channel that is still inoperable after completion of Required Action B.2 must be placed in trip if more than [48] hours have elapsed since the initial channel failure.

C.1 and C.2

The excore detectors are used to generate the internal ASI used as an input to the TM/LP and APD - High trips. Incore detectors provide a more accurate measurement of ASI. If one or more excore detectors cannot be calibrated to match incore detectors, power is restricted or reduced during subsequent operations because of increased uncertainty associated with using uncalibrated excore detectors.

The Completion Time of 24 hours is adequate to perform the SR while minimizing the risk of operating in an unsafe condition.

BASES

ACTIONS (continued)

D.1, D.2.1, D.2.2.1, and D.2.2.2

Condition D applies to one automatic bypass removal channel inoperable. If the bypass removal channel for any operating bypass cannot be restored to OPERABLE status, the associated RPS channel may be considered OPERABLE only if the bypass is not in effect. Otherwise, the affected RPS channel must be declared inoperable, as in Condition A, and the bypass either removed or the bypass removal channel repaired. The Bases for Required Actions and Completion Times are the same as discussed for Condition A.

E.1, E.2.1, and E.2.2

Condition E applies to two inoperable automatic bypass removal channels. If the bypass removal channels cannot be restored to OPERABLE status, the associated RPS channel may be considered OPERABLE only if the bypass is not in effect. Otherwise, the affected RPS channels must be declared inoperable, as in Condition B, and the bypass either removed or the bypass removal channel repaired. Also, Required Action E.2.2 provides for the restoration of the one affected automatic trip channel to OPERABLE status within the rules of Completion Time specified under Condition B. Completion Times are consistent with Condition B.

F.1

Condition F is entered when the Required Action and associated Completion Time of Conditions A, B, C, D, or E are not met for the Axial Power Distribution and Loss of Load Trip Functions.

If the Required Actions associated with these Conditions cannot be completed within the required Completion Times, the reactor must be brought to a MODE in which the Required Actions do not apply. The allowed Completion Time of 6 hours to reduce THERMAL POWER to < 15% RTP is reasonable, based on operating experience, to decrease power to < 15% RTP from full power conditions in an orderly manner and without challenging plant systems.

BASES

ACTIONS (continued)

G.1

Condition G is entered when the Required Action and associated Completion Time of Conditions A, B, C, D, E, or F are not met.

If the Required Actions associated with these Conditions cannot be completed within the required Completion Times, the reactor must be brought to a MODE in which the Required Actions do not apply. The allowed Completion Time of 6 hours to be in MODE 3 is reasonable, based on operating experience, for reaching the required MODE from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

The SRs for any particular RPS Function are found in the SR column of Table 3.3.1-1 for that Function. Most Functions are subject to CHANNEL CHECK, CHANNEL FUNCTIONAL TEST, CHANNEL CALIBRATION, and response time testing.

-----------------------------------REVIEWER'S NOTE-----------------------------------
In order for a plant to take credit for topical reports as the basis for justifying Frequencies, topical reports must be supported by an NRC staff SER that establishes the acceptability of each topical report for that plant (Ref. 9).

SR 3.3.1.1

Performance of the CHANNEL CHECK once every 12 hours ensures that gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the parameter indicated on one channel to a similar parameter on other channels. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value. Significant deviations between the two instrument channels could be an indication of excessive instrument drift in one of the channels or of something even more serious. CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying that the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

Agreement criteria are determined by the plant staff based on a combination of the channel instrument uncertainties, including indication and readability. If a channel is outside the criteria, it may be an indication that the transmitter or the signal processing equipment has drifted outside its limits.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The Frequency, about once every shift, is based on operating experience that demonstrates the rarity of channel failure. Since the probability of two random failures in redundant channels in any 12 hour period is extremely low, the CHANNEL CHECK minimizes the chance of loss of protective function due to failure of redundant channels. The CHANNEL CHECK supplements less formal, but more frequent, checks of channel OPERABILITY during normal operational use of the displays associated with the LCO required channels.

SR 3.3.1.2

A daily calibration (heat balance) is performed when THERMAL POWER is ≥ 20%. The daily calibration shall consist of adjusting the "nuclear power calibrate" potentiometers to agree with the calorimetric calculation if the absolute difference is > 1.5%. The "ΔT power calibrate" potentiometers are then used to null the "nuclear power - ΔT power" indicators on the RPS Reactor Power Calibration and Indication panel. Performance of the daily calibration ensures that the two inputs to the Q power measurement are indicating accurately with respect to the much more accurate secondary calorimetric calculation.

The Frequency of 24 hours is based on plant operating experience and takes into account indications and alarms located in the control room to detect deviations in channel outputs. The Frequency is modified by a Note indicating this Surveillance must be performed within 12 hours after THERMAL POWER is ≥ 20% RTP. The secondary calorimetric is inaccurate at lower power levels. The 12 hours allows time requirements for plant stabilization, data taking, and instrument calibration.

A second Note indicates the daily calibration may be suspended during PHYSICS TESTS. This ensures that calibration is proper preceding and following physics testing at each plateau, recognizing that during testing, changes in power distribution and RCS temperature may render the calorimetric inaccurate.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.1.3

It is necessary to calibrate the excore power range channel upper and lower subchannel amplifiers such that the internal ASI used in the TM/LP and APD - High trips reflects the true core power distribution as determined by the incore detectors. A Note to the Frequency indicates the Surveillance is required within 12 hours after THERMAL POWER is ≥ [20]% RTP. Uncertainties in the excore and incore measurement process make it impractical to calibrate when THERMAL POWER is < [20]% RTP. The Completion Time of 12 hours allows time for plant stabilization, data taking, and instrument calibration. If the excore detectors are not properly calibrated to agree with the incore detectors, power is restricted during subsequent operations because of increased uncertainty associated with using uncalibrated excore detectors. The 31 day Frequency is adequate, based on operating experience of the excore linear amplifiers and the slow burnup of the detectors. The excore readings are a strong function of the power produced in the peripheral fuel bundles and do not represent an integrated reading across the core. Slow changes in neutron flux during the fuel cycle can also be detected at this Frequency.

SR 3.3.1.4

A CHANNEL FUNCTIONAL TEST is performed on each RPS instrument channel, except Loss of Load and Power Rate of Change, every [92] days to ensure the entire channel will perform its intended function when needed. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

In addition to power supply tests, The RPS CHANNEL FUNCTIONAL TEST consists of three overlapping tests as described in Reference 8. These tests verify that the RPS is capable of performing its intended function, from bistable input through the RTCBs. They include:

BASES

SURVEILLANCE REQUIREMENTS (continued)

Bistable Tests

The bistable setpoint must be found to trip within the Allowable Values specified in the LCO and left set consistent with the assumptions of the plant specific setpoint analysis (Ref. 7). As found and as left values must also be recorded and reviewed for consistency with the assumptions of the frequency extension analysis. The requirements for this review are outlined in Reference 10.

A test signal is superimposed on the input in one channel at a time to verify that the bistable trips within the specified tolerance around the setpoint. This is done with the affected RPS channel trip channel bypassed. Any setpoint adjustment shall be consistent with the assumptions of the current plant specific setpoint analysis.

Matrix Logic Tests

Matrix Logic tests are addressed in LCO 3.3.3. This test is performed one matrix at a time. It verifies that a coincidence in the two input channels for each Function removes power from the matrix relays. During testing, power is applied to the matrix relay test coils and prevents the matrix relay contacts from assuming their de-energized state. This test will detect any short circuits around the bistable contacts in the coincidence logic, such as may be caused by faulty bistable relay or trip channel bypass contacts.

Trip Path Tests

Trip Path (Initiation Logic) tests are addressed in LCO 3.3.3. These tests are similar to the Matrix Logic tests, except that test power is withheld from one matrix relay at a time, allowing the initiation circuit to de-energize, opening the affected set of RTCBs. The RTCBs must then be closed prior to testing the other three initiation circuits, or a reactor trip may result.

The Frequency of [92] days is based on the reliability analysis presented in topical report CEN-327, "RPS/ESFAS Extended Test Interval Evaluation" (Ref. 10).

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.1.5

A CHANNEL CALIBRATION of the excore power range channels every 92 days ensures that the channels are reading accurately and within tolerance. The Surveillance verifies that the channel responds to a measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drift between successive calibrations to ensure that the channel remains operational between successive tests. CHANNEL CALIBRATIONS must be performed consistent with the plant specific setpoint analysis.

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the frequency extension analysis. The requirements for this review are outlined in Reference [10].

A Note is added stating that the neutron detectors are excluded from CHANNEL CALIBRATION because they are passive devices with minimal drift and because of the difficulty of simulating a meaningful signal. Slow changes in detector sensitivity are compensated for by performing the daily calorimetric calibration (SR 3.3.1.2) and the monthly linear subchannel gain check (SR 3.3.1.3). In addition, associated control room indications are continuously monitored by the operators.

The Frequency of 92 days is acceptable, based on plant operating experience, and takes into account indications and alarms available to the operator in the control room.

SR 3.3.1.6

A CHANNEL FUNCTIONAL TEST on the Loss of Load and Power Rate of Change channels is performed prior to a reactor startup to ensure the entire channel will perform its intended function if required. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions. The Loss of Load pressure sensor cannot be tested during reactor operation without closing the high pressure TSV, which would result in a turbine trip or reactor trip. The Power Rate of Change - High trip Function is required during startup operation and is bypassed when shut down or > 15% RTP.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.1.7

SR 3.3.1.7 is a CHANNEL FUNCTIONAL TEST similar to SR 3.3.1.4, except SR 3.3.1.7 is applicable only to bypass Functions and is performed once within 92 days prior to each startup. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions. Proper operation of bypass permissives is critical during plant startup because the bypasses must be in place to allow startup operation and must be removed at the appropriate points during power ascent to enable certain reactor trips. Consequently, the appropriate time to verify bypass removal function OPERABILITY is just prior to startup. The allowance to conduct this test within 92 days of startup is based on the reliability analysis presented in topical report CEN-327, "RPS/ESFAS Extended Test Interval Evaluation" (Ref. 10). Once the operating bypasses are removed, the bypasses must not fail in such a way that the associated trip Function gets inadvertently bypassed. This feature is verified by the trip Function CHANNEL FUNCTIONAL TEST, SR 3.3.1.4. Therefore, further testing of the bypass function after startup is unnecessary.

SR 3.3.1.8

SR 3.3.1.8 is the performance of a CHANNEL CALIBRATION every [18] months.

CHANNEL CALIBRATION is a complete check of the instrument channel including the sensor. The Surveillance verifies that the channel responds to a measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drift between successive calibrations to ensure that the channel remains operational between successive tests. CHANNEL CALIBRATIONS must be performed consistent with the plant specific setpoint analysis.

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the frequency extension analysis. The requirements for this review are outlined in Reference [10].

The Frequency is based upon the assumption of an 18 month calibration interval for the determination of the magnitude of equipment drift.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The Surveillance is modified by a Note to indicate that the neutron detectors are excluded from CHANNEL CALIBRATION because they are passive devices with minimal drift and because of the difficulty of simulating a meaningful signal. Slow changes in detector sensitivity are compensated for by performing the daily calorimetric calibration (SR 3.3.1.2) and the monthly linear subchannel gain check (SR 3.3.1.3).

SR 3.3.1.9

This SR ensures that the RPS RESPONSE TIMES are verified to be less than or equal to the maximum values assumed in the safety analysis. Individual component response times are not modeled in the analyses. The analyses model the overall or total elapsed time from the point at which the parameter exceeds the trip setpoint value at the sensor to the point at which the RTCBs open. Response times are conducted on an [18] month STAGGERED TEST BASIS. This results in the interval between successive surveillances of a given channel of n x 18 months, where n is the number of channels in the function. The Frequency of

[18] months is based upon operating experience, which has shown that random failures of instrumentation components causing serious response time degradation, but not channel failure, are infrequent occurrences. Also, response times cannot be determined at power, since equipment operation is required. Testing may be performed in one measurement or in overlapping segments, with verification that all components are tested.

----------------------------------REVIEWER'S NOTE----------------------------------
Applicable portions of the following TS Bases are applicable to plants adopting CEOG Topical Report CE NPSD-1167-1, "Elimination of Pressure Sensor Response Time Testing Requirements."

Response time may be verified by any series of sequential, overlapping or total channel measurements, including allocated sensor response time, such that the response time is verified. Allocations for sensor response times may be obtained from records of test results, vendor test data, or vendor engineering specifications. Topical Report CE NPSD-1167-A, "Elimination of Pressure Sensor Response Time Testing Requirements," (Ref. 11) provides the basis and methodology for using allocated sensor response times in the overall verification of the channel response time for specific sensors identified in the Topical Report. Response time verification for other sensor types must be demonstrated by test. The allocation of sensor response times must be verified prior to placing a new component in operation and reverified after maintenance that may adversely affect the sensor response time.

BASES

SURVEILLANCE REQUIREMENTS (continued)

A Note is added to indicate that the neutron detectors are excluded from RPS RESPONSE TIME testing because they are passive devices with minimal drift and because of the difficulty of simulating a meaningful signal. Slow changes in detector sensitivity are compensated for by performing the daily calorimetric calibration (SR 3.3.1.2).

REFERENCES

1. Regulatory Guide 1.105, Revision 3, "Setpoints for Safety-Related Instrumentation."
2. 10 CFR 50, Appendix A, GDC 21.
3. 10 CFR 100.
4. IEEE Standard 279-1971, April 5, 1972.
5. FSAR, Chapter [14].
6. 10 CFR 50.49.
7. "Plant Protection System Selection of Trip Setpoint Values."
8. FSAR, Section [7.2].
9. NRC Safety Evaluation Report, [Date].
10. CEN-327, June 2, 1986, including Supplement 1, March 3, 1989.
11. CEOG Topical Report CE NPSD-1167-A, "Elimination of Pressure Sensor Response Time Testing Requirements."

BASES

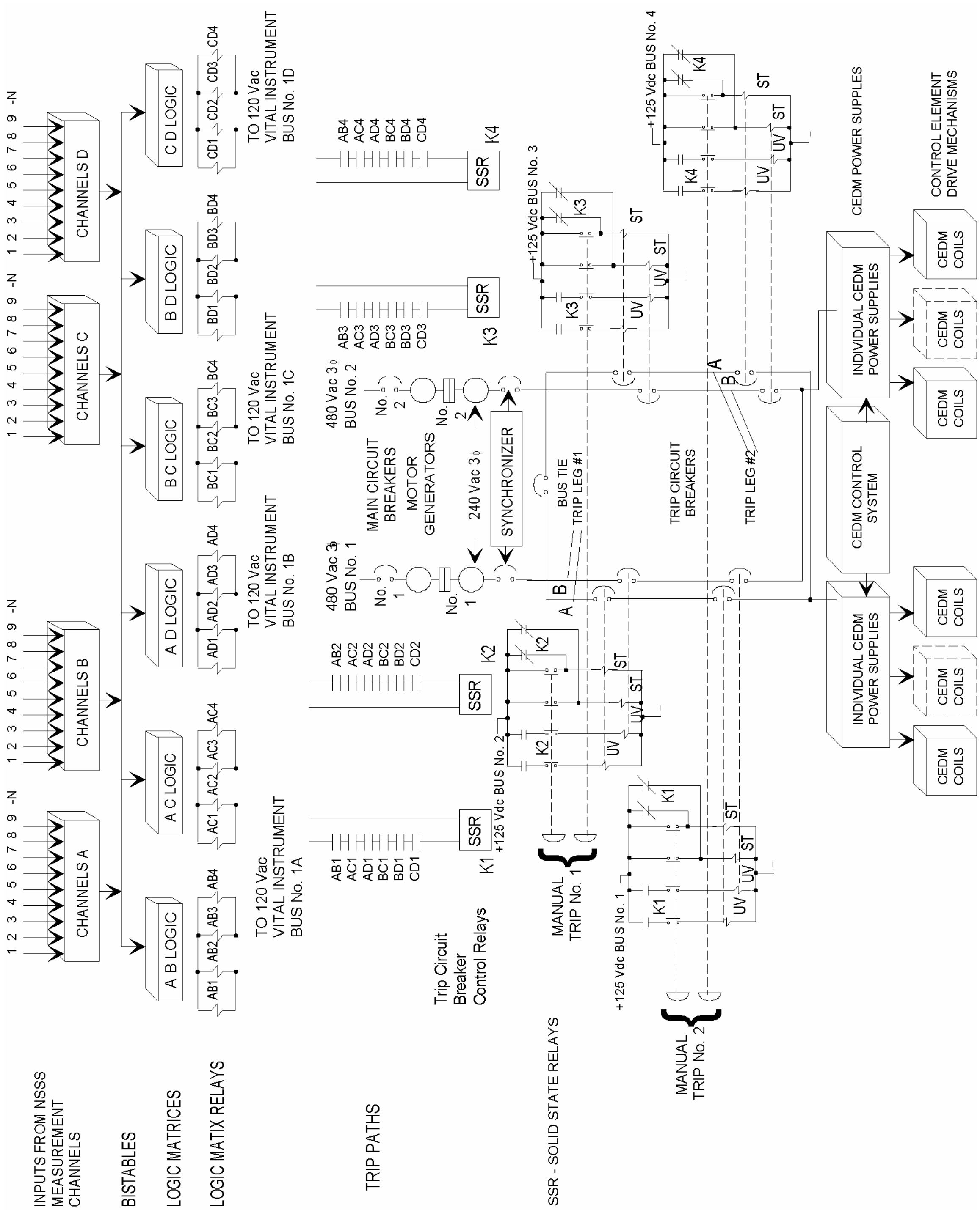


Figure B 3.3.1-1 (page 1 of 1)
Functional Diagram of the Two-Out-of-Four Logic and RTCB Configuration

B 3.3 INSTRUMENTATION

B 3.3.2 Reactor Protective System (RPS) Instrumentation - Shutdown (Analog)

BASES

BACKGROUND

The RPS initiates a reactor trip to protect against violating the core specified acceptable fuel design limits and reactor coolant pressure boundary integrity during anticipated operational occurrences (AOOs). By tripping the reactor, the RPS also assists the Engineered Safety Features systems in mitigating accidents.

The protection and monitoring systems have been designed to ensure safe operation of the reactor. This is achieved by specifying limiting safety system settings (LSSS) in terms of parameters directly monitored by the RPS, as well as LCOs on other reactor system parameters and equipment performance.

The LSSS, defined in this Specification as the Allowable Value, in conjunction with the LCOs, establish the threshold for protective system action to prevent exceeding acceptable limits during Design Basis Accidents.

During AOOs, which are those events expected to occur one or more times during the plant life, the acceptable limits are:

- The departure from nucleate boiling ratio shall be maintained above the Safety Limit (SL) value to prevent departure from nucleate boiling,
- Fuel centerline melting shall not occur, and
- The Reactor Coolant System pressure SL of 2750 psia shall not be exceeded.

Maintaining the parameters within the above values ensures that the offsite dose will be within the 10 CFR 50 (Ref. 1) and 10 CFR 100 (Ref. 2) criteria during AOOs.

Accidents are events that are analyzed even though they are not expected to occur during the plant life. The acceptable limit during accidents is that the offsite dose shall be maintained within an acceptable fraction of 10 CFR 100 (Ref. 2) limits. Different accident categories allow a different fraction of these limits based on probability of occurrence. Meeting the acceptable dose limit for an accident category is considered having acceptable consequences for that event.

BASES

BACKGROUND (continued)

The RPS is segmented into four interconnected modules. These modules are:

- Measurement channels,
- Bistable trip units,
- RPS Logic, and
- Reactor trip circuit breakers (RTCBs).

This LCO applies only to the Power Rate of Change - High trip Functions and associated instrument channels in MODES 3, 4, and 5 with any of the RTCBs closed and any Control Element Assembly (CEA) capable of being withdrawn. In MODES 1 and 2, this trip Function is addressed in LCO 3.3.1, "Reactor Protective System (RPS) Instrumentation - Operating." LCO 3.3.13, "[Logarithmic] Power Monitoring Channels," applies when the RTCBs are open or CEA Drive System is not capable of CEA withdrawal. In the case of LCO 3.3.13, the logarithmic power instrumentation channels are required for monitoring neutron flux, although the trip Function is not required.

<u>Measurement Channels and Trip Units</u>

The measurement channels providing input to the Power Rate of Change - High Function consist of wide range nuclear instrumentation channels using neutron flux leakage from the reactor vessel.

Other aspects of the Power Rate of Change - High trip are similar to the other measurement channels and bistable trip units. These are addressed in the Background section of LCO 3.3.1.

APPLICABLE SAFETY ANALYSES

Each of the analyzed accidents and transients can be detected by one or more RPS Functions. The accident analysis contained in Reference 3 takes credit for most RPS trip Functions. Functions not specifically credited in the accident analysis were qualitatively credited in the safety analysis and the NRC staff approved licensing basis for the plant. These Functions may provide protection for conditions that do not require dynamic transient analysis to demonstrate Function performance. Other Functions, such as the Loss of Load trip, are purely equipment protective, and their use minimizes the potential for equipment damage.

BASES

APPLICABLE SAFETY ANALYSES (continued)

The Power Rate of Change - High trip is used to trip the reactor when excore wide range power indicates an excessive rate of change.

The Power Rate of Change - High trip is not required for protection. It serves as a backup to the administratively enforced startup rate limit.

The Power Rate of Change - High Function minimizes transients for events such as a continuous CEA withdrawal or a boron dilution event from low power levels. The Power Rate of Change - High trip is automatically bypassed at < 1E-4% RTP, as sensed by the wide range nuclear instrument (NI) Level 2 bistable, when poor counting statistics may lead to erroneous indication. It is also bypassed at > 12% RTP, where moderator temperature coefficient and fuel temperature coefficient make high rate of change of power unlikely. This bypass is effected by the power range NI Level 1 bistable. Automatic bypass removal is also effected by these bistables. With the RTCBs open, the Power Rate of Change - High trip is not required to be OPERABLE; however, the indication and alarm Functions of at least two channels are required to be OPERABLE. LCO 3.3.13 ensures the wide range channels are available to detect and alert the operator to a boron dilution event.

The RPS instrumentation satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

The LCO requires all instrumentation performing an RPS Function to be OPERABLE. Failure of any required portion of the instrument channel or bypass removal channel renders the affected channel(s) inoperable and reduces the reliability of the affected Functions.

Actions allow maintenance (trip channel) bypass of individual channels, but the bypass activates interlocks that prevent operation with a second channel in the same Function bypassed. Plants are restricted to 48 hours in a trip channel bypass condition before either restoring the Function to four channel operation (two-out-of-four logic) or placing the channel in trip (one-out-of-three logic). At plants where adequate channel to channel independence has been demonstrated, specific exceptions have been approved by the NRC staff to permit one of the two-out-of-four channels to be bypassed for an extended period of time.

This LCO requires four channels of Power Rate of Change - High to be OPERABLE in MODES 3, 4, and 5, when the RTCBs are closed and the CEA Drive System is capable of CEA withdrawal. MODE 1 and 2 requirements are addressed in LCO 3.3.1. This trip is not credited in the safety analysis. Therefore, the Allowable Value specified in SR 3.3.4.2 is not derived from an analytical limit.

BASES

APPLICABILITY

This LCO is applicable to the Power Rate of Change - High reactor trip in MODES 3, 4 and 5. MODES 1 and 2 are addressed in LCO 3.3.1.

The power rate of change trip is required in MODES 3, 4, and 5, with the RTCBs closed and a CEA capable of being withdrawn to provide backup protection for boron dilution and CEA withdrawal events. The power rate of change trip is not credited in the safety analysis, but is part of the NRC approved licensing basis for the plant.

The power rate of change trip has operating bypasses discussed in the LCO section. In MODES 3, 4, and 5, the emphasis is placed on return to power events. The reactor is protected in these MODES by ensuring adequate SDM.

ACTIONS

The most common causes of channel inoperability are outright failure or drift of the bistable or process module sufficient to exceed the tolerance allowed by the plant specific setpoint analysis. Typically, the drift is found to be small and results in a delay of actuation rather than a total loss of function. This determination is generally made during the performance of a CHANNEL FUNCTIONAL TEST when the process instrument is set up for adjustment to bring it to within specification. If the trip setpoint is less conservative than the Allowable Value in Table 3.3.1-1, the channel is declared inoperable immediately, and the appropriate Condition(s) must be entered immediately.

In the event a channel's trip setpoint is found nonconservative with respect to the Allowable Value, or the transmitter, instrument loop, signal processing electronics, or RPS bistable is found inoperable, then all affected Functions provided by that channel must be declared inoperable and the plant must enter the Condition for the particular protection Function affected.

When the number of inoperable channels in a trip Function exceeds that specified in any related Condition associated with the same trip Function, then the plant is outside the safety analysis. Therefore, LCO 3.0.3 is immediately entered if applicable in the current MODE of operation.

<u>A.1, A.2.1, and A.2.2</u>

Condition A applies to the failure of a single channel of the Power Rate of Change - High RPS automatic trip Function.

BASES

ACTIONS (continued)

RPS coincidence logic is normally two-out-of-four. If one RPS bistable trip unit or associated instrument channel is inoperable, startup or power operation is allowed to continue, providing the inoperable trip unit is placed in bypass or trip within 1 hour (Required Action A.1). With one channel in bypass, no additional random failure of a single channel could spuriously trip the reactor and a valid trip signal can still trip the reactor. With one channel in trip, an additional random failure of a single channel could spuriously trip the reactor. Therefore, it is preferable to place an inoperable channel in bypass rather than trip.

The Completion Time of 1 hour allotted to restore, bypass, or trip the channel is sufficient to allow the operator to take all appropriate actions for the failed channel, while ensuring that the risk involved in operating with the failed channel is acceptable.

For plants that have not demonstrated sufficient channel to channel independence, the failed channel is restored to OPERABLE status or is placed in trip within 48 hours (Required Action A.2.1 or Required Action A.2.2). Required Action A.2.1 restores the full capability of the Function. Required Action A.2.2 places the Function in a one-out-of-three configuration. In this configuration, common cause failure of dependent channels cannot prevent trip.

The [48] hour Completion Time is based on operating experience, which has demonstrated that a random failure of a second channel occurring during the [48] hour period is a low probability event.

<u>B.1 and B.2</u>

Condition B applies to the failure of two channels in the Power Rate of Change - High RPS automatic trip Function.

Required Action B.1 provides for placing one inoperable channel in bypass and the other channel in trip within the Completion Time of 1 hour. This Completion Time is sufficient to allow the operator to take all appropriate actions for the failed channels, while ensuring the risk involved in operating with the failed channels is acceptable. With one channel of protective instrumentation bypassed, the RPS is in a two-out-of-three logic; but with another channel failed, the RPS may be operating in a two-out-of-two logic. This is outside the assumptions made in the analyses and should be corrected. To correct the problem, the second channel is placed in trip. This places the RPS in a one-out-of-two logic. If any of the other OPERABLE channels receives a trip signal, the reactor will trip.

BASES

ACTIONS (continued)

[The bypassed channel should be restored to OPERABLE status within 48 hours for reasons similar to those stated under Condition A. After one channel is restored to OPERABLE status, the provisions of Condition A still apply to the remaining inoperable channel. Therefore, the channel that is still inoperable after completion of Required Action B.2 shall be placed in trip if more than 48 hours have elapsed since the initial channel failure.]

C.1, C.2.1, C.2.2.1, and C.2.2.2

Condition C applies to one automatic bypass removal channel inoperable. If the bypass removal channel cannot be restored to OPERABLE status, the associated Power Rate of Change - High RPS channel may be considered OPERABLE only if the bypass is not in effect. Otherwise, the affected RPS channel must be declared inoperable, as in Condition A, and the bypass either removed or the bypass removal channel repaired. The Bases for the Required Actions and Completion Times are the same as discussed for Condition A.

D.1, D.2.1, and D.2.2

Condition D applies to two inoperable automatic bypass removal channels. If the bypass removal channels cannot be restored to OPERABLE status, the associated Power Rate of Change - High RPS channel may be considered OPERABLE only if the bypass is not in effect. Otherwise, the affected RPS channels must be declared inoperable, as in Condition B, and the bypass either removed or the bypass removal channel repaired. Also, Required Action D.2.2 provides for the restoration of the one affected automatic trip channel to OPERABLE status within the rules of Completion Time specified under Condition B. Completion Times are consistent with Condition B.

E.1

Condition E is entered when the Required Actions and associated Completion Times of Condition A, B, C, or D are not met.

BASES

ACTIONS (continued)

If Required Actions associated with these Conditions cannot be completed within the required Completion Time, opening the RTCBs brings the reactor to a MODE where the LCO does not apply and ensures no CEA withdrawal will occur. The basis for the Completion Time of 6 hours is that it is adequate to complete the Required Actions without challenging plant systems, including the insertion of CEAs for plants that normally maintain CEAs withdrawn when shut down.

SURVEILLANCE REQUIREMENTS

-----------------------------------REVIEWER'S NOTE-----------------------------------
In order for a plant to take credit for topical reports as the basis for justifying Frequencies, topical reports must be supported by an NRC staff Safety Evaluation Report that establishes the acceptability of each topical report for that plant.

SR 3.3.2.1

Performance of the CHANNEL CHECK on each wide range channel once every 12 hours ensures that gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the parameter indicated on one channel to a similar parameter on another channel. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value. Significant deviations between the two instrument channels could be an indication of excessive instrument drift in one of the channels or of something even more serious. CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying that the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

Agreement criteria are determined by the plant staff based on a combination of the channel instrument uncertainties, including isolation, indication, and readability. If a channel is outside the criteria, it may be an indication that the transmitter or the signal processing equipment has drifted outside its limits.

The Frequency, about once every shift, is based on operating experience that demonstrates the rarity of channel failure. Since the probability of two random failures in redundant channels in any 12 hour period is extremely low, the CHANNEL CHECK minimizes the chance of loss of protective function due to failure of redundant channels. The CHANNEL CHECK supplements less formal, but more frequent, checks of channel OPERABILITY during normal operational use of the displays associated with the LCO required channels.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.2.2

A CHANNEL FUNCTIONAL TEST on the power rate of change channels is performed once every 92 days to ensure the entire channel will perform its intended function if required. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions. The Power Rate of Change - High trip Function is required during startup operation and is bypassed when shut down or > 15% RTP. Additionally, operating experience has shown that these components usually pass the Surveillance when performed at a Frequency of once every 92 days prior to each reactor startup.

SR 3.3.2.3

SR 3.3.2.3 is a CHANNEL FUNCTIONAL TEST similar to SR 3.3.2.2, except SR 3.3.2.3 is applicable only to bypass Functions and is performed once within 92 days prior to each startup. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

Proper operation of bypass permissives is critical during plant startup because the bypasses must be in place to allow startup operation and must be removed at the appropriate points during power ascent to enable certain reactor trips. Consequently, the appropriate time to verify bypass removal function OPERABILITY is just prior to startup. The allowance to conduct this Surveillance within 92 days of startup is based on the reliability analysis presented in topical report CEN-327, "RPS/ESFAS Extended Test Interval Evaluation" (Ref. 5). Once the operating bypasses are removed, the bypasses must not fail in such a way that the associated trip Function gets inadvertently bypassed. This feature is verified by the trip Function CHANNEL FUNCTIONAL TEST, SR 3.3.2.2. Therefore, further testing of the bypass function after startup is unnecessary.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.2.4

SR 3.3.2.4 is the performance of a CHANNEL CALIBRATION every [18] months.

CHANNEL CALIBRATION is a complete check of the instrument channel including the sensor. The Surveillance verifies that the channel responds to a measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drift between successive calibrations to ensure that the channel remains operational between successive tests. CHANNEL CALIBRATIONS must be performed consistent with the plant specific setpoint analysis.

Only the Allowable Values are specified for each RPS trip Function. Nominal trip setpoints are specified in the plant specific setpoint calculations. The nominal setpoints are selected to ensure the setpoints measured by CHANNEL FUNCTIONAL TESTS do not exceed the Allowable Value if the bistable is performing as required. Operation with a trip setpoint less conservative than the nominal trip setpoint, but within its Allowable Value, is acceptable, provided that operation and testing are consistent with the assumptions of the plant specific setpoint calculations. Each Allowable Value specified is more conservative than the analytical limit assumed in the safety analysis in order to account for instrument uncertainties appropriate to the trip Function. These uncertainties are defined in the "Plant Protection System Selection of Trip Setpoint Values" (Ref. 4).

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the surveillance interval extension analysis. The requirements for this review are outlined in Reference 5.

The Frequency is based upon the assumption of an [18] month calibration interval in the determination of the magnitude of equipment drift.

The Surveillance is modified by a Note to indicate that the neutron detectors are excluded from CHANNEL CALIBRATION because they are passive devices with minimal drift and because of the difficulty of simulating a meaningful signal.

BASES

REFERENCES

1. 10 CFR 50, Appendix A.
2. 10 CFR 100.
3. FSAR, Chapter [14].
4. "Plant Protection System Selection of Trip Setpoint Values."
5. CEN-327, June 2, 1986, including Supplement 1, March 3, 1989.

B 3.3 INSTRUMENTATION

B 3.3.3 Reactor Protective System (RPS) Logic and Trip Initiation (Analog)

BASES

BACKGROUND

The RPS initiates a reactor trip to protect against violating the core specified acceptable fuel design limits and reactor coolant pressure boundary integrity during anticipated operational occurrences (AOOs). By tripping the reactor, the RPS also assists the Engineered Safety Features (ESF) systems in mitigating accidents.

The protection and monitoring systems have been designed to ensure safe operation of the reactor. This is achieved by specifying limiting safety system settings (LSSS) in terms of parameters directly monitored by the RPS, as well as LCOs on other reactor system parameters and equipment performance.

The LSSS, defined in this Specification as the Allowable Value, in conjunction with the LCOs, establish the threshold for protective system action to prevent exceeding acceptable limits during Design Basis Accidents.

During AOOs, which are those events expected to occur one or more times during the plant life, the acceptable limits are:

- The departure from nucleate boiling ratio shall be maintained above the Safety Limit (SL) value to prevent departure from nucleate boiling,
- Fuel centerline melting shall not occur, and
- The Reactor Coolant System pressure SL of 2750 psia shall not be exceeded.

Maintaining the parameters within the above values ensures that the offsite dose will be within the 10 CFR 50 (Ref. 1) and 10 CFR 100 (Ref. 2) criteria during AOOs.

Accidents are events that are analyzed even though they are not expected to occur during the plant life. The acceptable limit during accidents is that the offsite dose shall be maintained within an acceptable fraction of 10 CFR 100 (Ref. 2) limits. Different accident categories allow a different fraction of these limits based on probability of occurrence. Meeting the acceptable dose limit for an accident category is considered having acceptable consequences for that event.

BASES

BACKGROUND (continued)

The RPS is segmented into four interconnected modules. These modules are:

- Measurement channels,
- Bistable trip units,
- RPS Logic, and
- Reactor trip circuit breakers (RTCBs).

This LCO addresses the RPS Logic and RTCBs, including Manual Trip capability. LCO 3.3.1, "Reactor Protective System (RPS) Instrumentation - Operating," provides a description of the role of this equipment in the RPS. This is summarized below:

<u>RPS Logic</u>

The RPS Logic, consisting of Matrix and Initiation Logic, employs a scheme that provides a reactor trip when bistables in any two of the four channels sense the same input parameter trip. This is called a two-out-of-four trip logic. This logic and the RTCB configuration are shown in Figure B 3.3.1-1.

Bistable relay contact outputs from the four channels are configured into six logic matrices. Each logic matrix checks for a coincident trip in the same parameter in two bistable channels. The matrices are designated the AB, AC, AD, BC, BD, and CD matrices to reflect the bistable channels being monitored. Each logic matrix contains four normally energized matrix relays. When a coincidence is detected, consisting of a trip in the same Function in the two channels being monitored by the logic matrix, all four matrix relays de-energize.

The matrix relay contacts are arranged into trip paths, with one of the four matrix relays in each matrix opening contacts in one of the four trip paths. Each trip path provides power to one of the four normally energized RTCB control relays (K1, K2, K3, and K4). The trip paths thus each have six contacts in series, one from each matrix, and perform a logical <u>OR</u> function, opening the RTCBs if any one or more of the six logic matrices indicate a coincidence condition.

BASES

BACKGROUND (continued)

Each trip path is responsible for opening one set of two of the eight RTCBs. The RTCB control relays (K-relays), when de-energized, interrupt power to the breaker undervoltage trip attachments and simultaneously apply power to the shunt trip attachments on each of the two breakers. Actuation of either the undervoltage or shunt trip attachment is sufficient to open the RTCB and interrupt power from the motor generator (MG) sets to the control element drive mechanisms (CEDMs).

When a coincidence occurs in two RPS channels, all four matrix relays in the affected matrix de-energize. This in turn de-energizes all four breaker control relays, which simultaneously de-energize the undervoltage and energize the shunt trip attachments in all eight RTCBs, tripping them open.

The Initiation Logic consists of the trip path power source, matrix relays and their associated contacts, all interconnecting wiring, and solid state (auxiliary) relays through the K-relay contacts in the RTCB control circuitry.

It is possible to change the two-out-of-four RPS Logic to a two-out-of-three logic for a given input parameter in one channel at a time by trip channel bypassing select portions of the matrix logic. Trip channel bypassing a bistable effectively shorts the bistable relay contacts in the three matrices associated with that channel. Thus, the bistables will function normally, producing normal trip indication and annunciation, but a reactor trip will not occur unless two additional channels indicate a trip condition. Trip channel bypassing can be simultaneously performed on any number of parameters in any number of channels, providing each parameter is bypassed in only one channel at a time. An interlock prevents simultaneous trip channel bypassing of the same parameter in more than one channel. Trip channel bypassing is normally employed during maintenance or testing.

Reactor Trip Circuit Breakers (RTCBs)

The reactor trip switchgear, shown in Figure B 3.3.1-1, consists of eight RTCBs, which are operated in four sets of two breakers (four channels). Power input to the reactor trip switchgear comes from two full capacity MG sets operated in parallel such that the loss of either MG set does not de-energize the CEDMs. There are two separate CEDM power supply

BASES

BACKGROUND (continued)

buses, each bus powering half of the CEDMs. Power is supplied from the MG sets to each bus via two redundant paths (trip legs). Trip legs 1A and 1B supply power to CEDM bus 1. Trip legs 2A and 2B supply power to CEDM bus 2. This ensures that a fault or the opening of a breaker in one trip leg (i.e., for testing purposes) will not interrupt power to the CEDM buses.

Each of the four trip legs consists of two RTCBs in series. The two RTCBs within a trip leg are actuated by separate initiation circuits.

The eight RTCBs are operated as four sets of two breakers (four channels). For example, if a breaker receives an open signal in trip leg A (for CEDM bus 1), an identical breaker in trip leg B (for CEDM bus 2) will also receive an open signal. This arrangement ensures that power is interrupted to both CEDM buses, thus preventing trip of only half of the control element assemblies (CEAs) (a half trip). Any one inoperable breaker in a channel will make the entire channel inoperable.

Each set of RTCBs is operated by either a Manual Trip push button or an RPS actuated K-relay. There are four Manual Trip push buttons, arranged in two sets of two, as shown in Figure B 3.3.1-1. Depressing both push buttons in either set will result in a reactor trip.

When a Manual Trip is initiated using the control room push buttons, the RPS trip paths and K-relays are bypassed, and the RTCB undervoltage and shunt trip attachments are actuated independent of the RPS.

Manual Trip circuitry includes the push button and interconnecting wiring to both RTCBs necessary to actuate both the undervoltage and shunt trip attachments, but excludes the K-relay contacts and their interconnecting wiring to the RTCBs, which are considered part of the Initiation Logic.

Functional testing of the entire RPS, from bistable input through the opening of individual sets of RTCBs, can be performed either at power or shutdown and is normally performed on a quarterly basis. FSAR, Section [7.2] (Ref. 3), explains RPS testing in more detail.

APPLICABLE SAFETY ANALYSES

Reactor Protective System (RPS) Logic

The RPS Logic provides for automatic trip initiation to maintain the SLs during AOOs and assist the ESF systems in ensuring acceptable consequences during accidents. All transients and accidents that call for a reactor trip assume the RPS Logic is functioning as designed.

BASES

APPLICABLE SAFETY ANALYSES (continued)

Reactor Trip Circuit Breakers (RTCBs)

All of the transient and accident analyses that call for a reactor trip assume that the RTCBs operate and interrupt power to the CEDMs.

Manual Trip

There are no accident analyses that take credit for the Manual Trip; however, the Manual Trip is part of the RPS circuitry. It is used by the operator to shut down the reactor whenever any parameter is rapidly trending toward its trip setpoint. A Manual Trip accomplishes the same results as any one of the automatic trip Functions.

The RPS Logic and initiation satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

Reactor Protective System (RPS) Logic

Failures of individual bistable relays and their contacts are addressed in LCO 3.3.1. This Specification addresses failures of the Matrix Logic not addressed in the above, such as the failure of matrix relay power supplies or the failure of the trip channel bypass contact in the bypass condition.

Loss of a single vital bus will de-energize one of the two power supplies in each of three matrices. This will result in four RTCBs opening; however, the remaining four closed RTCBs will prevent a reactor trip. For the purposes of this LCO, de-energizing up to three matrix power supplies due to a single failure is to be treated as a single channel failure, providing the affected matrix relays de-energize as designed, opening the affected RTCBs.

Each of the four Initiation Logic channels opens one set of RTCBs if any of the six coincidence matrices de-energize their associated matrix relays. They thus perform a logical OR function. Each Initiation Logic channel has its own power supply and is independent of the others. An Initiation Logic channel includes the matrix relay through to the K-relay contacts, which open the RTCB.

It is possible for two Initiation Logic channels affecting the same trip leg to de-energize if a matrix power supply or vital instrument bus fails. This will result in opening the two affected sets of RTCBs.

BASES

LCO (continued)

If one set of RTCBs has been opened in response to a single RTCB channel, Initiation Logic channel, or Manual Trip channel failure, the affected set of RTCBs may be closed for up to 1 hour for Surveillance on the OPERABLE Initiation Logic, RTCB, and Manual Trip channels. In this case, the redundant set of RTCBs will provide protection if a trip should be required. It is unlikely that a trip will be required during the Surveillance, coincident with a failure of the remaining series RTCB channel. If a single matrix power supply or vital bus failure has opened two sets of RTCBs, Manual Trip and RTCB testing on the closed breakers cannot be performed without causing a trip.

1. Matrix Logic

   This LCO requires six channels of Matrix Logic to be OPERABLE in MODES 1 and 2, and in MODES 3, 4, and 5 when any RTCB is closed and any CEA is capable of being withdrawn.

2. Initiation Logic

   This LCO requires four channels of Initiation Logic to be OPERABLE in MODES 1 and 2, and in MODES 3, 4, and 5 when any RTCB is closed and any CEA is capable of being withdrawn.

3. Reactor Trip Circuit Breakers (RTCBs)

   The LCO requires four RTCB channels to be OPERABLE in MODES 1 and 2, as well as in MODES 3, 4, and 5 when any RTCB is closed and any CEA is capable of being withdrawn.

   Each channel consists of two breakers operated in a single set by the Initiation Logic or Manual Trip circuitry. This ensures that power is interrupted at identical locations in the trip legs for both CEDM buses, thus preventing power removal to only one CEDM bus (a half trip).

   Failure of a single breaker affects the entire channel, and both breakers in the set must be opened. Without reliable RTCBs and associated support circuitry, a reactor trip cannot occur whether initiated automatically or manually.

   Each channel of RTCBs starts at the contacts actuated by the K-relay, and the contacts actuated by the Manual Trip, for each set of breakers. The K-relay actuated contacts and the upstream circuitry are considered to be RPS Logic. Manual Trip contacts and upstream circuitry are considered to be Manual Trip circuitry.

BASES

LCO (continued)

A Note associated with the ACTIONS states that if one set of RTCBs has been opened in response to a single RTCB channel, Initiation Logic channel, or Manual Trip channel failure, the affected set of RTCBs may be closed for up to 1 hour for Surveillance on the OPERABLE Initiation Logic, RTCB, and Manual Trip channels. In this case, the redundant set of RTCBs will provide protection. If a single matrix power supply or vital bus failure has opened two sets of RTCBs, Manual Trip and RTCB testing on the closed breakers cannot be performed without causing a trip. This Note is not applicable to Condition A, with one Matrix Logic channel inoperable.

4. Manual Trip

The LCO requires all four Manual Trip channels to be OPERABLE in MODES 1 and 2, and MODES 3, 4, and 5 when any RTCB is closed and any CEA is capable of being withdrawn.

Two independent sets of two adjacent push buttons are provided at separate locations. Each push button is considered a channel and operates two of the eight RTCBs. Depressing both push buttons in either set will cause an interruption of power to the CEDMs, allowing the CEAs to fall into the core. This design ensures that no single failure in any push button circuit can either cause or prevent a reactor trip.

APPLICABILITY

The RPS Matrix Logic, RTCBs, and Manual Trip are required to be OPERABLE in any MODE when any CEA is capable of being withdrawn from the core (i.e., RTCBs closed and power available to the CEDMs). This ensures the reactor can be tripped when necessary, but allows for maintenance and testing when the reactor trip is not needed.

In MODES 3, 4, and 5 with all the RTCBs open, the CEAs are not capable of withdrawal and these Functions do not have to be OPERABLE. However, two [logarithmic] power level channels must be OPERABLE to ensure proper indication of neutron population and to indicate a boron dilution event. This is addressed in LCO 3.3.13, "[Logarithmic] Power Monitoring Channels."

ACTIONS

When the number of inoperable channels in a trip Function exceeds that specified in any related Condition associated with the same trip Function, then the plant is outside the safety analysis. Therefore, LCO 3.0.3 is immediately entered if applicable in the current MODE of operation.

BASES

ACTIONS (continued)

A.1

Condition A applies if one Matrix Logic channel is inoperable or three Matrix Logic channels are inoperable due to a common power source failure de-energizing three matrix power supplies, in any applicable MODE. Loss of a single vital instrument bus will de-energize one of the two matrix power supplies in up to three matrices. This is considered a single matrix failure, providing the matrix relays associated with the failed power supplies de-energize as required.

Failure of the matrix relays to de-energize in all three affected matrices could, when combined with trip channel bypassing of bistable relay contacts in the other matrices, result in loss of RPS function.

The channel must be restored to OPERABLE status within 48 hours. The Completion Time of 48 hours provides the operator time to take appropriate actions and still ensures that any risk involved in operating with a failed channel is acceptable. Operating experience has demonstrated that the probability of a random failure of a second Matrix Logic channel is low during any given 48 hour interval. If the channel cannot be restored to OPERABLE status within 48 hours, Condition E is entered.

B.1

Condition B applies to one Initiation Logic channel, RTCB channel, or Manual Trip channel in MODES 1 and 2, since they have the same actions. MODES 3, 4, and 5, with the RTCBs shut, are addressed in Condition C. These Required Actions require opening the affected RTCBs. This removes the need for the affected channel by performing its associated safety function. With the RTCB open, the affected Functions are in one-out-of-two logic, which meets redundancy requirements, but testing on the OPERABLE channels cannot be performed without causing a reactor trip unless the RTCBs in the inoperable channels are closed to permit testing.

Required Action B.1 provides for opening the RTCBs associated with the inoperable channel within a Completion Time of 1 hour. This Required Action is conservative, since depressing the Manual Trip push button associated with either set of breakers in the other trip leg will cause a reactor trip. With this configuration, a single channel failure will not prevent a reactor trip. The allotted Completion Time is adequate to open the affected RTCBs while maintaining the risk of having them closed at an acceptable level.

BASES

ACTIONS (continued)

C.1

Condition C applies to the failure of one Initiation Logic channel, RTCB channel, or Manual Trip channel affecting the same trip leg in MODE 3, 4, or 5 with the RTCBs closed. The channel must be restored to OPERABLE status within 48 hours. If the inoperable channel cannot be restored to OPERABLE status within 48 hours, the affected RTCBs must be opened. In some cases, this condition may effect all of the RTCBs. This removes the need for the affected channel by performing its associated safety function. With the RTCBs open, the affected functions are in a one-out-of-two logic, which meets redundancy requirements.

The Completion Time of 48 hours is consistent with that of other RPS instrumentation and should be adequate to repair most failures.

Testing on the OPERABLE channels cannot be performed without causing a reactor trip unless the RTCBs in the inoperable channels are closed to permit testing.

D.1

Condition D applies to the failure of both Manual Trip or Initiation Logic channels affecting the same trip leg. Since this will open two channels of RTCBs, this Condition is also applicable to the two affected channels of RTCBs. This Condition allows for loss of a single vital instrument bus or matrix power supply, which will de-energize both Initiation Logic channels in the same trip leg. This will open both sets of RTCBs in the affected trip leg, satisfying the Required Action of opening the affected RTCBs.

Of greater concern is the failure of the initiation circuit in a nontrip condition (e.g., due to two initiation K-relay failures). With only one Initiation Logic channel failed in a nontrip condition, there is still the redundant set of RTCBs in the trip leg. With both failed in a nontrip condition, the reactor will not trip automatically when required. In either case, the affected RTCBs must be opened immediately by using the appropriate Manual Trip push buttons, since each of the four push buttons opens one set of RTCBs, independent of the initiation circuitry. Caution must be exercised, since depressing the wrong push buttons may result in a reactor trip.

BASES

ACTIONS (continued)

If two Manual Trip channels are inoperable and affecting the same trip leg, the associated RTCBs must be opened immediately to ensure Manual Trip capability is maintained. With the affected RTCBs open, any one of two Manual Trip push buttons being depressed will result in a reactor trip.

If the affected RTCB(s) cannot be opened, Condition E is entered. This would only occur if there is a failure in the Manual Trip circuitry or the RTCB(s).

E.1 and E.2

Condition E is entered if Required Actions associated with Condition A, B, or D are not met within the required Completion Time or if for one or more Functions more than one Manual Trip, Matrix Logic, Initiation Logic, or RTCB channel is inoperable for reasons other than Condition A or D.

If the RTCBs associated with the inoperable channel cannot be opened, the reactor must be shut down within 6 hours and all the RTCBs opened. A Completion Time of 6 hours is reasonable, based on operating experience, to reach the required MODE from full power conditions in an orderly manner and without challenging plant systems and to open RTCBs. All RTCBs should then be opened, placing the plant in a MODE where the LCO does not apply and ensuring no CEA withdrawal occurs.

SURVEILLANCE REQUIREMENTS

-----------------------------------REVIEWER'S NOTE-----------------------------------
In order for a plant to take credit for topical reports as the basis for justifying Frequencies, topical reports must be supported by an NRC staff Safety Evaluation Report that establishes the acceptability of each topical report for that unit (Ref. 4).

SR 3.3.3.1

A CHANNEL FUNCTIONAL TEST is performed on each RTCB channel every 31 days. This verifies proper operation of each RTCB. The RTCB must then be closed prior to testing the other RTCBs, or a reactor trip may result. The Frequency of 31 days is based on the reliability analysis presented in Topical Report CEN-327, "RPS/ESFAS Extended Test Interval Evaluation," (Ref. 5).

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.3.2

A CHANNEL FUNCTIONAL TEST on each RPS Logic channel is performed every [92] days to ensure the entire channel will perform its intended function when needed. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

In addition to power supply tests, the RPS CHANNEL FUNCTIONAL TEST consists of three overlapping tests as described in Reference 3. These tests verify that the RPS is capable of performing its intended function, from bistable input through the RTCBs. The first test, the bistable test, is addressed by SR 3.3.1.4 in LCO 3.3.1.

This SR addresses the two tests associated with the RPS Logic: Matrix Logic and Trip Path.

Matrix Logic Tests

These tests are performed one matrix at a time. They verify that a coincidence in the two input channels for each Function removes power from the matrix relays. During testing, power is applied to the matrix relay test coils and prevents the matrix relay contacts from assuming their de-energized state. The Matrix Logic tests will detect any short circuits around the bistable contacts in the coincidence logic such as may be caused by faulty bistable relay or trip channel bypass contacts.

Trip Path Tests

These tests are similar to the Matrix Logic tests, except that test power is withheld from one matrix relay at a time, allowing the initiation circuit to de-energize, opening the affected set of RTCBs. The RTCBs must then be closed prior to testing the other three initiation circuits, or a reactor trip may result.

The Frequency of [92] days is based on the reliability analysis presented in topical report CEN-327, "RPS/ESFAS Extended Test Interval Evaluation" (Ref. 5).

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.3.3

A CHANNEL FUNCTIONAL TEST on the Manual Trip channels is performed prior to a reactor startup to ensure the entire channel will perform its intended function if required. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions. The Manual Trip Function can be tested either at power or shutdown. However, the simplicity of this circuitry and the absence of drift concern makes this Frequency adequate. Additionally, operating experience has shown that these components usually pass the Surveillance when performed once within 7 days prior to each reactor startup.

[SR 3.3.3.4

Each RTCB is actuated by an undervoltage coil and a shunt trip coil. The system is designed so that either de-energizing the undervoltage coil or energizing the shunt trip coil will cause the circuit breaker to open. When an RTCB is opened, either during an automatic reactor trip or by using the manual push buttons in the control room, the undervoltage coil is de-energized and the shunt trip coil is energized. This makes it impossible to determine if one of the coils or associated circuitry is defective.

Therefore, once every 18 months, a CHANNEL FUNCTIONAL TEST is performed that individually tests all four sets of undervoltage coils and all four sets of shunt trip coils. During undervoltage coil testing, the shunt trip coils shall remain de-energized, preventing their operation. Conversely, during shunt trip coil testing, the undervoltage coils shall remain energized, preventing their operation. This Surveillance ensures that every undervoltage coil and every shunt trip coil is capable of performing its intended function and that no single active failure of any RTCB component will prevent a reactor trip. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical

BASES

SURVEILLANCE REQUIREMENTS (continued)

Specifications tests at least once per refueling interval with applicable extensions. The 18 month Frequency is based on the need to perform this Surveillance under the conditions that apply during a plant outage and the potential for an unplanned transient if the Surveillance were performed with the reactor at power. Operating experience has shown these components usually pass the Surveillance when performed at the Frequency of once every 18 months.

If one set of RTCBs has been opened in response to a single RTCB channel, Initiation Logic channel, or Manual Trip channel failure, the affected set of RTCBs may be closed for up to 1 hour for Surveillance on the OPERABLE Initiation Logic, RTCB, and Manual Trip channels. In this case, the redundant set of RTCBs will provide protection if a trip should be required. It is unlikely that a trip will be required during the Surveillance, coincident with a failure of the remaining series RTCB channel. If a single matrix power supply or vital bus failure has opened two sets of RTCBs, Manual Trip and RTCB testing on the closed breakers cannot be performed without causing a trip.]

REFERENCES

1. 10 CFR 50, Appendix A.
2. 10 CFR 100.
3. FSAR, Section [7.2].
4. NRC Safety Evaluation Report, [Date].
5. CEN-327, June 2, 1986, including Supplement 1, March 3, 1989.

B 3.3 INSTRUMENTATION

B 3.3.4 Engineered Safety Features Actuation System (ESFAS) Instrumentation (Analog)

BASES

BACKGROUND

The ESFAS initiates necessary safety systems, based upon the values of selected unit parameters, to protect against violating core design limits and the Reactor Coolant System (RCS) pressure boundary and to mitigate accidents.

The ESFAS contains devices and circuitry that generate the following signals when the monitored variables reach levels that are indicative of conditions requiring protective action:

1. Safety Injection Actuation Signal (SIAS),
2. Containment Spray Actuation Signal (CSAS),
3. Containment Isolation Actuation Signal (CIAS),
4. Main Steam Isolation Signal (MSIS),
5. Recirculation Actuation Signal (RAS), and
6. Auxiliary Feedwater Actuation Signal (AFAS).

Equipment actuated by each of the above signals is identified in the FSAR (Ref. 1).

Each of the above ESFAS actuation systems is segmented into four sensor subsystems and two actuation subsystems. Each sensor subsystem includes measurement channels and bistables. The actuation subsystems include two logic subsystems for sequentially loading the diesel generators.

Each of the four sensor subsystem channels monitors redundant and independent process measurement channels. Each sensor is monitored by at least one bistable. The bistable associated with each ESFAS Function will trip when the monitored variable exceeds the trip setpoint. When tripped, the sensor subsystems provide outputs to the two actuation subsystems.

BASES

BACKGROUND (continued)

The two independent actuation subsystems compare the four sensor subsystem outputs. If a trip occurs in the same parameter in two or more sensor subsystem channels, the two-out-of-four logic in each actuation subsystem will initiate one train of ESFAS. Each train can provide protection to the public in the case of a Design Basis Event. Actuation Logic is addressed in LCO 3.3.5, "Engineered Safety Features Actuation System (ESFAS) Logic and Manual Trip."

Each of the four sensor subsystems is mounted in a separate cabinet, excluding the sensors and field wiring.

The role of the sensor subsystem (measurement channels and bistables) is discussed below; actuation subsystems are discussed in LCO 3.3.5.

Measurement Channels

Measurement channels, consisting of field transmitters or process sensors and associated instrumentation, provide a measurable electronic signal based upon the physical characteristics of the parameter being measured.

Four identical measurement channels with electrical and physical separation are provided for each parameter used in the generation of trip signals. These are designated Channels A through D. Measurement channels provide input to ESFAS bistables within the same ESFAS channel. In addition, some measurement channels may also be used as inputs to Reactor Protective System (RPS) bistables, and most provide indication in the control room. Measurement channels used as an input to the RPS or ESFAS are not used for control Functions.

When a channel monitoring a parameter indicates an unsafe condition, the bistable monitoring the parameter in that channel will trip. Tripping two or more channels of bistables monitoring the same parameter will de-energize both channels of Actuation Logic of the associated Engineered Safety Features (ESF) equipment.

Three of the four measurement and bistable channels are necessary to meet the redundancy and testability of GDC 21 in Appendix A to 10 CFR 50 (Ref. 2). The fourth channel provides additional flexibility by allowing one channel to be removed from service (trip channel bypass) for maintenance or testing while still maintaining a minimum two-out-of-three logic.

BASES

BACKGROUND (continued)

In order to take full advantage of the four channel design, adequate channel to channel independence must be demonstrated, and approved by the NRC staff. Plants not currently licensed as to credit four channel independence that may desire this capability must have approval of the NRC staff documented by an NRC Safety Evaluation Report (Ref. 3). Adequate channel to channel independence includes physical and electrical independence of each channel from the others. Furthermore, each channel must be energized from separate inverters and station batteries. Plants not demonstrating four channel independence may operate in a two-out-of-three logic configuration for 48 hours.

Since no single failure will either cause or prevent a protective system actuation and no protective channel feeds a control channel, this arrangement meets the requirements of IEEE Standard 79-1971 (Ref. 4).

<u>Bistable Trip Units</u>

Bistable trip units receive an analog input from the measurement channels, compare the analog input to trip setpoints, and provide contact output to the Actuation Logic. They also provide local trip indication and remote annunciation.

There are four channels of bistables, designated A through D, for each ESF Function, one for each measurement channel. In cases where two ESF Functions share the same input and trip setpoint (e.g., containment pressure input to CSAS, CIAS, and SIAS and a Pressurizer Pressure - Low input to the RPS and SIAS), the same bistable may be used to satisfy both Functions.

The trip setpoints and Allowable Values used in the bistables are based on the analytical limits stated in Reference 5. The selection of these trip setpoints is such that adequate protection is provided when all sensor and processing time delays are taken into account. To allow for calibration tolerances, instrumentation uncertainties, instrument drift, and severe environment effects, for those ESFAS channels that must function in harsh environments as defined by 10 CFR 50.49 (Ref. 6), Allowable Values specified in Table 3.3.4-1, in the accompanying LCO, are conservatively adjusted with respect to the analytical limits. A detailed description of the method used to calculate the trip setpoints, including their explicit uncertainties, is provided in the "Plant Protection System Selection of Trip Setpoint Values" (Ref. 7). The actual nominal trip

BASES

BACKGROUND (continued)

setpoint entered into the bistable is normally still more conservative than that specified by the Allowable Value to account for changes in random measurement errors detectable by a CHANNEL FUNCTIONAL TEST. If the measured setpoint does not exceed the Allowable Value, the bistable is considered OPERABLE.

Setpoints in accordance with the Allowable Value will ensure that Safety Limits of Chapter 2.0, "SAFETY LIMITS (SLs)," are not violated during anticipated operational occurrences (AOOs) and that the consequences of Design Basis Accidents (DBAs) will be acceptable, providing the plant is operated from within the LCOs at the onset of the AOO or DBA and the equipment functions as designed.

ESFAS Logic

It is possible to change the two-out-of-four ESFAS logic to a two-out-of-three logic for a given input parameter in one channel at a time by disabling one channel input to the logic. Thus, the bistables will function normally, producing normal trip indication and annunciation, but ESFAS actuation will not occur since the bypassed channel is effectively removed from the coincidence logic. Trip channel bypassing can be simultaneously performed on any number of parameters in any number of channels, providing each parameter is bypassed in only one channel at a time. At some plants an interlock prevents simultaneous trip channel bypassing of the same parameter in more than one channel. Trip channel bypassing is normally employed during maintenance or testing.

ESFAS Logic is addressed in LCO 3.3.5.

APPLICABLE SAFETY ANALYSES

Each of the analyzed accidents can be detected by one or more ESFAS Functions. One of the ESFAS Functions is the primary actuation signal for that accident. An ESFAS Function may be the primary actuation signal for more than one type of accident. An ESFAS Function may also be a secondary, or backup, actuation signal for one or more other accidents. Functions such as Manual Initiation, not specifically credited in the accident analysis, serve as backups to Functions and are part of the NRC approved licensing basis for the plant.

ESFAS protective Functions are as follows:

BASES

APPLICABLE SAFETY ANALYSES (continued)

1. Safety Injection Actuation Signal

The SIAS ensures acceptable consequences during loss of coolant accident (LOCA) events, including steam generator tube rupture, and main steam line breaks (MSLBs) or feedwater line breaks (FWLBs) (inside containment). To provide the required protection, either a high containment pressure or a low pressurizer pressure signal will initiate SIAS. SIAS initiates the Emergency Core Cooling Systems (ECCS), control room isolation, and several other Functions, such as starting the emergency diesel generators.

2. Containment Spray Actuation Signal

The CSAS initiates containment spray, preventing containment overpressurization during a LOCA or MSLB. At some plants, both a high containment pressure signal and an SIAS have to actuate to provide the required protection. This configuration reduces the likelihood of inadvertent containment spray.

3. Containment Isolation Actuation Signal

The CIAS actuates the Containment Isolation System, ensuring acceptable consequences during LOCAs and MSLBs or FWLBs (inside containment). To provide protection, a high containment pressure signal will initiate CIAS at the same setpoint at which an SIAS is generated.

4. Main Steam Isolation Signal

The MSIS ensures acceptable consequences during an MSLB or FWLB by isolating both steam generators if either generator indicates a low steam generator pressure. The MSIS, concurrent with or following a reactor trip, minimizes the rate of heat extraction and subsequent cooldown of the RCS during these events.

BASES

APPLICABLE SAFETY ANALYSES (continued)

5. Recirculation Actuation Signal

At the end of the injection phase of a LOCA, the refueling water tank (RWT) will be nearly empty. Continued cooling must be provided by the ECCS to remove decay heat. The source of water for the ECCS pumps is automatically switched to the containment recirculation sump. Switchover from RWT to the containment sump must occur before the RWT empties to prevent damage to the ECCS pumps and a loss of core cooling capability. For similar reasons, switchover must not occur before there is sufficient water in the containment sump to support pump suction. Furthermore, early switchover must not occur to ensure sufficient borated water is injected from the RWT to ensure the reactor remains shut down in the recirculation mode. An RWT Level - Low signal initiates the RAS.

6. Auxiliary Feedwater Actuation Signal

An AFAS initiates feedwater flow to both steam generators if a low level is indicated in either steam generator, unless the generator is ruptured.

The AFAS maintains a steam generator heat sink during the following events:

- MSLB,
- FWLB,
- Inadvertent opening of a steam generator atmospheric dump valve, and
- Loss of feedwater.

A low steam generator water level signal will initiate auxiliary feed to the affected steam generator.

Secondary steam generator (SG) differential pressure (SG-A > SG-B) or (SG-B > SG-A) inhibits auxiliary feed to a generator identified as being ruptured. This input to the AFAS logic prevents loss of the intact generator while preventing feeding a ruptured generator during MSLBs and FWLBs. This prevents containment overpressurization during these events.

The ESFAS satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO

The LCO requires all channel components necessary to provide an ESFAS actuation to be OPERABLE.

The Bases for the LCO on ESFAS Functions are:

1. Safety Injection Actuation Signal

a. Containment Pressure - High

This LCO requires four channels of SIAS Containment Pressure - High to be OPERABLE in MODES 1, 2, and 3.

The Allowable Value for this trip is set high enough to allow for small pressure increases in containment expected during normal operation (i.e., plant heatup) and is not indicative of an offnormal condition. The setting is low enough to initiate the ESF Functions when an offnormal condition is indicated. This allows the ESF systems to perform as expected in the accident analyses to mitigate the consequences of the analyzed accidents.

b. Pressurizer Pressure - Low

This LCO requires four channels of SIAS Pressurizer Pressure - Low to be OPERABLE in MODES 1, 2, and 3.

The Allowable Value for this trip is set low enough to prevent actuating the SIAS during normal plant operation and pressurizer pressure transients. The setting is high enough that with a LOCA or MSLB it will actuate to perform as expected, mitigating the consequences of the accidents.

The Pressurizer Pressure - Low trip may be blocked when pressurizer pressure is reduced during controlled plant shutdowns. This block is permitted below 1800 psia, and block permissive responses are annunciated in the control room. This allows for a controlled depressurization of the RCS, while maintaining administrative control of ESF protection. From a blocked condition, the block will be automatically removed as pressurizer pressure increases above 1800 psia, as sensed by two of the four sensor subsystems, in accordance with the bypass philosophy of removing bypasses when the enabling conditions are no longer satisfied.

This LCO requires four channels of the bypass permissive removal for SIAS Pressurizer Pressure - Low to be OPERABLE in MODES 1, 2, and 3.

BASES

LCO (continued)

The bypass permissive channels consist of four sensor subsystems and two actuation subsystems. This LCO applies to failures in the four sensor subsystems, including sensors, bistables, and associated equipment. Failures in the actuation subsystems, including the manual bypass key switches, are considered Actuation Logic failures and are addressed in LCO 3.3.5.

This LCO applies to the bypass removal feature only. If the bypass enable Function is failed so as to prevent entering a bypass condition, operation may continue.

The block permissive is set low enough so as not to be enabled during normal plant operation, but high enough to allow blocking prior to reaching the trip setpoint.

2. Containment Spray Actuation Signal

CSAS is initiated either manually or automatically. At many plants, it is also necessary to have an automatic or manual SIAS for complete actuation. The SIAS opens the containment spray valves, whereas the CSAS actuates other required components. The SIAS requirement should always be satisfied on a legitimate CSAS, since the Containment Pressure - High signal setpoint used in the SIAS is the same setpoint used in the CSAS. At many plants, the transmitters used to initiate CSAS are independent of those used in the SIAS to prevent inadvertent containment spray due to failures in two sensor channels.

a. Containment Pressure - High

This LCO requires four channels of CSAS Containment Pressure - High to be OPERABLE in MODES 1, 2, and 3.

The Allowable Value is set high enough to allow for small pressure increases in containment expected during normal operation (i.e., plant heatup) and is not indicative of an offnormal condition. The setting is low enough to initiate the ESF Functions when an offnormal condition is indicated. This allows the ESF systems to perform as expected in the accident analyses to mitigate the consequences of the analyzed accidents.

BASES

LCO (continued)

The Containment Pressure - High setpoint is the same in the SIAS (Function 1), CSAS (Function 2), and CIAS (Function 3). However, different sensors and logic are used in each of these Functions.

3. Containment Isolation Actuation Signal

   a. Containment Pressure - High

   This LCO requires four channels of CIAS Containment Pressure - High to be OPERABLE in MODES 1, 2, and 3.

   The Allowable Value is set high enough to allow for small pressure increases in containment expected during normal operation (i.e., plant heatup) and is not indicative of an offnormal condition. The setting is low enough to initiate the ESF Functions when an offnormal condition is indicated. This allows the ESF systems to perform as expected in the accident analyses to mitigate the consequences of the analyzed accidents.

   The Containment Pressure - High setpoint is the same in the SIAS (Function 1), CSAS (Function 2), and CIAS (Function 3). However, different sensors and logic are used in each of these Functions.

   b. Containment Radiation - High

   This LCO requires four channels of CIAS Containment Radiation - High to be OPERABLE in MODES 1, 2, and 3.

   The Allowable Value is high enough to avoid unnecessary actuation, but adequate to provide diverse actuation of the CIAS in the event of a LOCA.

4. Main Steam Isolation Signal

   The MSIS is required to be OPERABLE in MODES 1, 2, and 3 except when all associated valves are closed and de-activated.

BASES

LCO (continued)

a. <u>Steam Generator Pressure - Low</u>

This LCO requires four channels of MSIS Steam Generator Pressure - Low for each steam generator to be OPERABLE in MODES 1, 2, and 3.

The Allowable Value is set below the full load operating value for steam pressure so as not to interfere with normal plant operation. However, the setting is high enough to provide the required protection for excessive steam demand. An excessive steam demand causes the RCS to cool down, resulting in a positive reactivity addition to the core. An MSIS is required to prevent the excessive cooldown.

This Function may be manually blocked when steam generator pressure is reduced during controlled plant cooldowns. The block is permitted below 785 psia, and block permissive responses are annunciated in the control room. This allows a controlled depressurization of the secondary system, while maintaining administrative control of ESF protection. From a blocked condition, the block will be removed automatically as steam generator pressure increases above 785 psia, as sensed by two of the four sensor subsystems, in accordance with the bypass philosophy of removing bypasses when the enabling conditions are no longer satisfied.

This LCO requires four channels per steam generator of the bypass removal for MSIS Steam Generator Pressure - Low to be OPERABLE in MODES 1, 2, and 3.

The bypass removal channels consist of four sensor subsystems and two actuation subsystems. This LCO applies to failures in the four sensor subsystems, including sensors, bistables, and associated equipment. Failures in the actuation subsystems, including the manual bypass key switches, are considered Actuation Logic failures and are addressed in LCO 3.3.5.

This LCO applies to the bypass removal feature only. If the bypass enable Function is failed so as to prevent entering a bypass condition, operation may continue.

The block permissive is set low enough so as not to be enabled during normal plant operation, but high enough to allow blocking prior to reaching the trip setpoint.

BASES

LCO (continued)

5. Recirculation Actuation Signal

a. Refueling Water Tank Level - Low

This LCO requires four channels of RWT Level - Low to be OPERABLE in MODES 1, 2, and 3.

The upper limit on the Allowable Value for this trip is set low enough to ensure RAS does not initiate before sufficient water is transferred to the containment sump. Premature recirculation could impair the reactivity control Function of safety injection by limiting the amount of boron injection. Premature recirculation could also damage or disable the recirculation system if recirculation begins before the sump has enough water to prevent air containment in the suction. The lower limit on the RWT Level - Low trip Allowable Value is high enough to transfer suction to the containment sump prior to emptying the RWT.

6. Auxiliary Feedwater Actuation Signal

The AFAS logic actuates auxiliary feedwater (AFW) to a steam generator on low level in that generator unless it has been identified as being ruptured.

A low level in either generator, as sensed by a two-out-of-four coincidence of four wide range sensors for any generator, will generate an AFAS start signal, which starts both trains of AFW pumps and feeds both steam generators. The AFAS also monitors the secondary differential pressure in both steam generators and initiates an AFAS block signal to a ruptured generator, if the pressure in that generator is lower than that in the other generator by the differential pressure setpoint.

a. Steam Generator A/B Level - Low

This LCO requires four channels for each steam generator of Steam Generator Level - Low to be OPERABLE in MODES 1, 2, and 3.

The Allowable Value ensures adequate time exists to initiate AFW while the steam generators can function as a heat sink.

BASES

LCO (continued)

b. Steam Generator Pressure Difference - High (SG-A > SG-B) or (SG-B > SG-A)

This LCO requires four channels per steam generator of Steam Generator Pressure Difference - High to be OPERABLE in MODES 1, 2, and 3.

The Allowable Value for this trip is high enough to allow for small pressure differences and normal instrumentation errors between the steam generator channels during normal operation without an actuation. The setting is low enough to detect and inhibit feeding of a ruptured steam generator in the event of an MSLB or FWLB, while permitting the feeding of the intact steam generator.

APPLICABILITY

All ESFAS Functions are required to be OPERABLE in MODES 1, 2, and 3. In MODES 1, 2, and 3 there is sufficient energy in the primary and secondary systems to warrant automatic ESF System responses to:

- Close the main steam isolation valves to preclude a positive reactivity addition,
- Actuate AFW to preclude the loss of the steam generators as a heat sink (in the event the normal feedwater system is not available),
- Actuate ESF systems to prevent or limit the release of fission product radioactivity to the environment by isolating containment and limiting the containment pressure from exceeding the containment design pressure during a design basis LOCA or MSLB, and
- Actuate ESF systems to ensure sufficient borated inventory to permit adequate core cooling and reactivity control during a design basis LOCA or MSLB accident.

In MODES 4, 5, and 6, automatic actuation of ESFAS Functions is not required because adequate time is available for plant operators to evaluate plant conditions and respond by manually operating the ESF components, if required, as addressed by LCO 3.3.5. In LCO 3.3.5, manual capability is required for Functions other than AFAS in MODE 4, even though automatic actuation is not required. Because of the large number of components actuated on each ESFAS, actuation is simplified by the use of the Manual Trip push buttons. Manual Trip of AFAS is not required in MODE 4 because AFW or shutdown cooling will already be in operation in this MODE.

BASES

APPLICABILITY (continued)

The ESFAS Actuation Logic must be OPERABLE in the same MODES as the automatic and Manual Trip. In MODE 4, only the portion of the ESFAS logic responsible for the required Manual Trip must be OPERABLE.

In MODES 5 and 6, ESFAS initiated systems are either reconfigured or disabled for shutdown cooling operation. Accidents in these MODES are slow to develop and would be mitigated by manual operation of individual components.

ACTIONS

The most common cause of channel inoperability is outright failure or drift of the bistable or process module sufficient to exceed the tolerance allowed by the plant specific setpoint analysis.

Typically, the drift is small and results in a delay of actuation rather than a total loss of function. Determination of setpoint drift is generally made during the performance of a CHANNEL FUNCTIONAL TEST when the process instrument is set up for adjustment to bring it to within specification. If the actual trip setpoint is not within the Allowable Value in Table 3.3.4-1, the channel is inoperable and the appropriate Condition(s) are entered.

In the event a channel's trip setpoint is found nonconservative with respect to the Allowable Value in Table 3.3.4-1, or the sensor, instrument loop, signal processing electronics, or ESFAS bistable is found inoperable, then all affected Functions provided by that channel must be declared inoperable and the plant must enter the Condition statement for the particular protection Function affected.

When the number of inoperable channels in a trip Function exceeds those specified in any related Condition associated with the same trip Function, then the plant is outside the safety analysis. Therefore, LCO 3.0.3 should be immediately entered if applicable in the current MODE of operation.

A Note has been added to clarify the application of the Completion Time rules. The Conditions of this Specification may be entered independently for each Function in Table 3.3.4-1. Completion Times for the inoperable channel of a Function will be tracked separately.

BASES

ACTIONS (continued)

[A.1

Condition A applies to one CSAS Containment Pressure - High channel inoperable. CSAS logic is identical to that of the other ESFAS Functions; however, the inadvertent actuation of a CSAS is undesirable, since it may damage equipment inside containment. For this reason, placing the inoperable channel in trip is not an option as it is in Conditions B and C.]

[For those plants in which the SIAS is required for a complete CSAS actuation, Condition B for one ESFAS channel inoperable and Condition C for two ESFAS channels inoperable may be preferable to Condition A.

If one CSAS channel is inoperable, operation is allowed to continue, providing the inoperable channel is placed in bypass within 1 hour. The Completion Time of 1 hour allotted to bypass the channel is sufficient to allow the operator to take all appropriate actions for the failed channel and still ensures that the risk involved in operating with the failed channel is acceptable.]

B.1, B.2.1, and B.2.2

Condition B applies to the failure of a single channel of one or more input parameters in the following ESFAS Functions:

1. Safety Injection Actuation Signal
   Containment Pressure - High
   Pressurizer Pressure – Low

3. Containment Isolation Actuation Signal
   Containment Pressure - High
   Containment Radiation - High

4. Main Steam Isolation Signal
   Steam Generator Pressure - Low

5. Recirculation Actuation Signal
   Refueling Water Tank Level - Low

6. Auxiliary Feedwater Actuation Signal
   Steam Generator Level - Low
   Steam Generator Pressure Difference - High

BASES

ACTIONS (continued)

ESFAS coincidence logic is normally two-out-of-four. If one ESFAS channel is inoperable, startup or power operation is allowed to continue as long as action is taken to restore the design level of redundancy.

If one ESFAS channel is inoperable, startup or power operation is allowed to continue, providing the inoperable channel is placed in bypass or trip within 1 hour (Required Action B.1). With one channel in bypass, no additional random failure of a single channel could spuriously trip the reactor and a valid trip signal can still trip the reactor. With one channel in trip, an additional random failure of a single channel could spuriously trip the reactor. Therefore, it is preferable to place an inoperable channel in bypass rather than trip.

The Completion Time of 1 hour allotted to bypass or trip the channel is sufficient to allow the operator to take all appropriate actions for the failed channel and still ensures that the risk involved in operating with the failed channel is acceptable.

One failed channel is restored to OPERABLE status or is placed in trip within [48] hours (Required Action B.2.1 or B.2.2). Required Action B.2.1 restores the full capability of the function. Required Action B.2.2 places the function in a one-out-of-three configuration. In this configuration, common cause failure of the dependent channel cannot prevent ESFAS actuation. The [48] hour Completion Time is based upon operating experience, which has demonstrated that a random failure of a second channel occurring during the [48] hour period is a low probability event.

<u>C.1 and C.2</u>

Condition C applies to the failure of two channels in any of the following ESFAS functions:

1. Safety Injection Actuation Signal
   Containment Pressure - High
   Pressurizer Pressure - Low

3. Containment Isolation Actuation Signal
   Containment Pressure - High
   Containment Radiation - High

4. Main Steam Isolation Signal
   Steam Generator Pressure - Low

BASES

ACTIONS (continued)

5. Recirculation Actuation Signal
   Refueling Water Tank Level - Low

6. Auxiliary Feedwater Actuation Signal
   Steam Generator Level - Low
   Steam Generator Pressure Difference - High

With two inoperable channels, one channel should be placed in bypass, and the other channel should be placed in trip within the 1 hour Completion Time. With one channel of protective instrumentation bypassed, the ESFAS Function is in two-out-of-three logic, but with another channel failed the ESFAS may be operating with a two-out-of-two logic. This is outside the assumptions made in the analyses and should be corrected. To correct the problem, the second channel is placed in trip. This places the ESFAS in a one-out-of-two logic. If any of the other OPERABLE channels receives a trip signal, ESFAS actuation will occur.

One of the failed channels should be restored to OPERABLE status within [48] hours, for reasons similar to those stated under Condition B. After one channel is restored to OPERABLE status, the provisions of Condition B still apply to the remaining inoperable channel. Therefore, the channel that is still inoperable after completion of Required Action C.2 must be placed in trip if more than [48] hours has elapsed since the initial channel failure.

D.1, D.2.1, D.2.2.1, and D.2.2.2

Condition D applies to the failure of one bypass removal channel.

The bypass removal channels consist of four sensor subsystems and two actuation subsystems. Condition D applies to failures in one of the four sensor subsystems, including sensors, bistables, and associated equipment. Failures in the actuation subsystems, including the manual bypass key switches, are considered Actuation Logic failures and are addressed in LCO 3.3.5.

In Condition D, it is permissible to continue operation with one bypass permissive removal channel failed, providing the bypass is disabled (Required Action D.1). This can be accomplished by removing the bypass with the manual bypass key switch, which disables the bypass in both trains. Since the bypass Function must be manually enabled, the bypass permissive Function will not by itself cause an undesired bypass insertion.

BASES

ACTIONS (continued)

Alternatively, the bypass may be disabled by defeating the bypass permissive input in one of the four channels to the two-out-of-four bypass removal logic, placing the bypass removal feature in one-out-of-three logic. Thus, any of the remaining three channels is capable of removing the bypass feature when the bypass enable conditions are no longer valid.

If the bypass removal feature in the inoperable channel cannot be defeated, actions to address the inoperability of the affected automatic trip channel must be taken. Required Action D.2.1, Required Action D.2.2.1, and Required Action D.2.2.2 are equivalent to the Required Actions for a single automatic trip channel failure (Condition B). The 1 hour and [48] hour Completion Times have the same bases as discussed for Condition B.

<u>E.1, E.2.1, and E.2.2</u>

Condition E applies to two inoperable bypass removal channels. The bypass removal channels consist of four sensor subsystems and two actuation subsystems. This Condition applies to failures in two of the four sensor subsystems. With two of the four sensor subsystems failed in a nonconservative direction (enabling the bypass Function), the bypass removal feature is in two-out-of-two logic. Failures in the actuation subsystems, including the manual bypass key switches, are considered Actuation Logic failures and are addressed in LCO 3.3.5.

In Condition E, it is permissible to continue operation with two bypass permissive channels failed, providing the bypasses are disabled in a similar manner as discussed for Condition D.

If the failed bypasses cannot be disabled, actions to address the inoperability of the affected automatic trip channels must be taken. Required Action E.2.1 and Required Action E.2.2 are equivalent to the Required Actions for a two automatic trip channel failure (Condition C). Also similar to Condition C, after one set of inoperable channels is restored, the provisions of Condition D still apply to the remaining inoperable channel, with the Completion Time measured from the point of the initial bypass channel failure. The 1 hour and [48] hour Completion Times have the same bases as discussed for Condition C.

BASES

ACTIONS (continued)

F.1 and F.2

If the Required Actions and associated Completion Times of Condition A, B, C, D, or E are not met, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 4 within [12] hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

The SRs for any particular ESFAS Function are found in the SRs column of Table 3.3.4-1 for that Function. Most functions are subject to CHANNEL CHECK, CHANNEL FUNCTIONAL TEST, CHANNEL CALIBRATION, and response time testing.

----------------------------------REVIEWER'S NOTE-----------------------------------
In order for a unit to take credit for topical reports as the basis for justifying Frequencies, topical reports should be supported by an NRC staff Safety Evaluation Report that establishes the acceptability of each topical report for that unit.

SR 3.3.4.1

Performance of the CHANNEL CHECK once every 12 hours ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the parameter indicated on one channel to a similar parameter on other channels. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value. Significant deviations between instrument channels could be an indication of excessive instrument drift in one of the channels or of something even more serious. CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

Agreement criteria are determined by the plant staff based on a combination of the channel instrument uncertainties, including indication and readability. If a channel is outside the criteria, it may be an indication that the sensor or the signal processing equipment has drifted outside its limit. If the channels are within the criteria, it is an indication that the channels are OPERABLE. If the channels are normally off scale during

BASES

SURVEILLANCE REQUIREMENTS (continued)

times when Surveillance is required, the CHANNEL CHECK will only verify that they are off scale in the same direction. Offscale low current loop channels are verified to be reading at the bottom of the range and not failed downscale.

The Frequency of about once every shift is based on operating experience that demonstrates channel failure is rare. Since the probability of two random failures in redundant channels in any 12 hour period is extremely low, the CHANNEL CHECK minimizes the chance of loss of protective function due to failure of redundant channels. The CHANNEL CHECK supplements less formal, but more frequent, checks of CHANNEL OPERABILITY during normal operational use of displays associated with the LCO required channels.

SR 3.3.4.2

A CHANNEL FUNCTIONAL TEST is performed every [92] days to ensure the entire channel will perform its intended function when needed. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

The CHANNEL FUNCTIONAL TEST tests the individual sensor subsystems using an analog test input to each bistable.

A test signal is superimposed on the input in one channel at a time to verify that the bistable trips within the specified tolerance around the setpoint. Any setpoint adjustment shall be consistent with the assumptions of the current plant specific setpoint analysis.

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the surveillance interval extension analysis. The requirements for this review are outlined in Reference [8].

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.4.3

SR 3.3.4.3 is a CHANNEL FUNCTIONAL TEST similar to SR 3.3.4.2, except 3.3.4.3 is performed within 92 days prior to startup and is only applicable to bypass Functions. These include the Pressurizer Pressure - Low bypass and the MSIS Steam Generator Pressure - Low bypass. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

The CHANNEL FUNCTIONAL TEST for proper operation of the bypass removal Functions is critical during plant heatups because the bypasses may be in place prior to entering MODE 3 but must be removed at the appropriate points during plant startup to enable the ESFAS Function. Consequently, just prior to startup is the appropriate time to verify bypass removal Function OPERABILITY. Once the bypasses are removed, the bypasses must not fail in such a way that the associated ESFAS Function is inappropriately bypassed. This feature is verified by the appropriate ESFAS Function CHANNEL FUNCTIONAL TEST.

The allowance to conduct this Surveillance within 92 days of startup is based upon the reliability analysis presented in topical report CEN-327, "RPS/ESFAS Extended Test Interval Evaluation" (Ref. 9).

SR 3.3.4.4

CHANNEL CALIBRATION is a complete check of the instrument channel, including the sensor. The Surveillance verifies that the channel responds to a measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drift between successive calibrations to ensure that the channel remains operational between successive surveillances. CHANNEL CALIBRATIONS must be performed consistent with the plant specific setpoint analysis.

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the extension analysis. The requirements for this review are outlined in Reference [8].

BASES

SURVEILLANCE REQUIREMENTS (continued)

The Frequency is based upon the assumption of an [18] month calibration interval for the determination of the magnitude of equipment drift in the setpoint analysis.

SR 3.3.4.5

This Surveillance ensures that the train actuation response times are the maximum values assumed in the safety analyses. Individual component response times are not modeled in the analyses. The analysis models the overall or total elapsed time, from the point at which the parameter exceeds the trip setpoint value at the sensor to the point at which the equipment in both trains reaches the required functional state (e.g., pumps at rated discharge pressure, valves in full open or closed position). Response time testing acceptance criteria are included in Reference 3. The test may be performed in one measurement or in overlapping segments, with verification that all components are measured.

-----------------------------------REVIEWER'S NOTE-----------------------------------
Applicable portions of the following TS Bases are applicable to plants adopting CEOG Topical Report CE NPSD-1167-1, "Elimination of Pressure Sensor Response Time Testing Requirements."

Response time may be verified by any series of sequential, overlapping or total channel measurements, including allocated sensor response time, such that the response time is verified. Allocations for sensor response times may be obtained from records of test results, vendor test data, or vendor engineering specifications. Topical Report CE NPSD-1167-A, "Elimination of Pressure Sensor Response Time Testing Requirements," (Ref. 10) provides the basis and methodology for using allocated sensor response times in the overall verification of the channel response time for specific sensors identified in the Topical Report. Response time verification for other sensor types must be demonstrated by test. The allocation of sensor response times must be verified prior to placing a new component in operation and reverified after maintenance that may adversely affect the sensor response time.

BASES

SURVEILLANCE REQUIREMENTS (continued)

ESF RESPONSE TIME tests are conducted on a STAGGERED TEST BASIS of once every [18] months. This results in the interval between successive tests of a given channel of n x 18 months, where n is the number of channels in the Function. Surveillance of the final actuation devices, which make up the bulk of the response time, is included in the testing of each channel. Therefore, staggered testing results in response time verification of these devices every [18] months. The [18] month STAGGERED TEST BASIS Frequency is based upon plant operating experience, which shows that random failures of instrumentation components causing serious response time degradation, but not channel failure, are infrequent occurrences.

REFERENCES

1. FSAR, Section [7.3].
2. 10 CFR 50, Appendix A.
3. NRC Safety Evaluation Report, [Date].
4. IEEE Standard 279-1971.
5. FSAR, Chapter [14].
6. 10 CFR 50.49.
7. "Plant Protection System Selection of Trip Setpoint Values."
8. FSAR, Section [7.2].
9. CEN-327, June 2, 1986, including Supplement 1, March 3, 1989.
10. CEOG Topical Report CE NPSD-1167-A, "Elimination of Pressure Sensor Response Time Testing Requirements."

B 3.3 INSTRUMENTATION

B 3.3.5 Engineered Safety Features Actuation System (ESFAS) Logic and Manual Trip (Analog)

BASES

BACKGROUND

The ESFAS initiates necessary safety systems, based upon the values of selected unit parameters, to protect against violating core design limits and the Reactor Coolant System (RCS) pressure boundary and to mitigate accidents.

The ESFAS contains devices and circuitry that generate the following signals when the monitored variables reach levels that are indicative of conditions requiring protective action:

1. Safety Injection Actuation Signal (SIAS),
2. Containment Spray Actuation Signal (CSAS),
3. Containment Isolation Actuation Signal (CIAS),
4. Main Steam Isolation Signal (MSIS),
5. Recirculation Actuation Signal (RAS), and
6. Auxiliary Feedwater Actuation Signal (AFAS).

Equipment actuated by each of the above signals is identified in the FSAR (Ref. 1).

Each of the above ESFAS actuation systems is segmented into four sensor subsystems addressed by LCO 3.3.4, "Engineered Safety Features Actuation System (ESFAS) Instrumentation," and two actuation subsystems addressed by this LCO. Each sensor subsystem includes measurement channels and bistables. The SIAS actuation subsystems include two logic subsystems for sequentially loading the diesel generators.

Each of the four sensor subsystem channels monitors redundant and independent process measurement channels. Each sensor is monitored by at least one bistable. The bistable associated with each ESFAS Function will trip when the monitored variable exceeds the trip setpoint. When tripped, the sensor subsystems provide outputs to the two actuation subsystems.

BASES

BACKGROUND (continued)

The two independent actuation subsystems each compare the four associated sensor subsystem outputs. If a trip occurs in two or more sensor subsystem channels, the two-out-of-four logic in each actuation subsystem will initiate one train of ESFAS. Each has sufficient equipment to provide protection to the public in the case of a Design Basis Event. The sensor subsystem is addressed in LCO 3.3.4. This LCO addresses the actuation subsystem.

Each of the four sensor subsystems is mounted in a separate cabinet, excluding the sensors and field wiring.

The role of the sensor subsystem (measurement channels and bistables) is discussed in LCO 3.3.4. That of the actuation subsystem is discussed below.

<u>ESFAS Logic</u>

The two independent actuation subsystems compare the four sensor subsystem outputs. If a trip occurs in the same parameter in two or more sensor subsystem channels, the two-out-of-four logic in each actuation subsystem initiates one train of ESFAS. Either train controls sufficient redundant and independent equipment.

Each actuation subsystem channel is housed in two cabinets. One cabinet contains the logic circuitry for the actuation channel, while the other cabinet contains the power relay equipment. This power relay equipment includes the power relays (initiation relays) that actuate the ESFAS equipment in response to a signal from the Actuation Logic.

It is possible to change the two-out-of-four ESFAS Logic to a two-out-of-three logic for a given input parameter in one channel at a time by disabling one channel input to the logic. Thus, the bistables will function normally, producing normal trip indication and annunciation, but ESFAS actuation will not occur since the bypassed channel is effectively removed from the coincidence logic. Maintenance bypassing can be simultaneously performed on any number of parameters in any number of channels, providing each parameter is bypassed in only one channel at a time. At some plants an interlock prevents simultaneous maintenance bypassing of the same parameter in more than one channel. Maintenance bypassing is normally employed during maintenance or testing.

BASES

BACKGROUND (continued)

For plants that have demonstrated sufficient channel to channel independence, two-out-of-three logic is the minimum that is required to provide adequate plant protection, since a failure of one channel still ensures that ESFAS actuation would be generated by the two remaining OPERABLE channels. Two-out-of-three logic also prevents inadvertent actuation caused by any single channel failure in a trip condition.

In addition to the maintenance bypasses, there are operating bypasses (blocks) on the Pressurizer Pressure - Low input to the SIAS and on the Steam Generator Pressure - Low input to the MSIS when these inputs are no longer required for protection. These bypasses are enabled manually when the enabling conditions are satisfied in three of the four sensor subsystem channels. The operating bypass circuitry employs four bistable channels in the sensor subsystems, sensing pressurizer pressure (for the SIAS) and steam generator pressure (for the MSIS). These bistables provide contact output to the three-out-of-four logic in the two actuation subsystem channels. When the logic is satisfied, manual bypassing is permitted. There are two manual bypass actuation controls for each Function, one per train.

All operating bypasses are automatically removed when enabling bypass conditions are no longer satisfied.

Manual ESFAS initiation capability is provided to permit the operator to manually actuate an Engineered Safety Features (ESF) System when necessary. Two push buttons are provided in the control room for each ESFAS Function. Each push button actuates one train via the ESFAS Logic.

The Actuation Logic is tested by inserting a local test signal. A coincidence logic trip will occur if there is the simultaneous presence of a sensor channel trip, either legitimate or due to testing. Most ESFAS Functions employ several separate parallel two-out-of-four Actuation Logic modules, with each module actuating a subset of the ESFAS equipment associated with that Function. Each of these subchannels can be tested individually so that simultaneous actuation of an entire train can be avoided during testing.

Except in the case of actuation subchannels SIAS Nos. 5 and 10, CIAS No. 5, and MSIS No. 1, all Actuation Logic channels can be tested at power. The above designated subchannels must be tested when shut down because they actuate the following equipment, which cannot be actuated at power:

BASES

BACKGROUND (continued)

- Reactor coolant pump (RCP) seal bleedoff isolation valves,
- Service water isolation valves,
- Volume control tank (VCT) discharge valves,
- Letdown stop valves,
- Component cooling water (CCW) to RCPs,
- CCW from RCPs,
- Main steam isolation valves (MSIVs),
- Feedwater isolation valves, and
- Instrument air containment isolation valves.

APPLICABLE SAFETY ANALYSES

Each of the analyzed accidents can be detected by one or more ESFAS Functions. One of the ESFAS Functions is the primary actuation signal for that accident. An ESFAS Function may be the primary actuation signal for more than one type of accident. An ESFAS Function may also be a secondary, or backup, actuation signal for one or more other accidents. Functions such as Manual Initiation, not specifically credited in the accident analysis, serve as backups to Functions and are part of the NRC staff approved licensing basis for the plant.

ESFAS protective Functions are as follows:

1. Safety Injection Actuation Signal

   The SIAS ensures acceptable consequences during loss of coolant accident (LOCA) events, including steam generator tube rupture, and main steam line breaks (MSLBs) or feedwater line breaks (FWLBs) (inside containment). To provide the required protection, either a high containment pressure or a low pressurizer pressure signal will initiate SIAS. SIAS initiates the Emergency Core Cooling Systems (ECCS) and performs several other Functions, such as initiating control room isolation and starting the diesel generators.

BASES

APPLICABLE SAFETY ANALYSES (continued)

2. Containment Spray Actuation Signal

The CSAS initiates containment spray, preventing containment overpressurization during a LOCA or MSLB. At some plants, both a high containment pressure signal and an SIAS have to actuate to provide the required protection. This configuration reduces the likelihood of inadvertent containment spray.

3. Containment Isolation Actuation Signal

The CIAS actuates the Containment Isolation System, ensuring acceptable consequences during LOCAs and MSLBs or FWLBs (inside containment). To provide protection, a high containment pressure signal will initiate CIAS at the same setpoint at which an SIAS is initiated.

4. Main Steam Isolation Signal

The MSIS ensures acceptable consequences during an MSLB or FWLB by isolating both steam generators if either generator indicates a low steam generator pressure. The MSIS, concurrent with or following a reactor trip, minimizes the rate of heat extraction and subsequent cooldown of the RCS during these events.

5. Recirculation Actuation Signal

At the end of the injection phase of a LOCA, the refueling water tank (RWT) will be nearly empty. Continued cooling must be provided by the ECCS to remove decay heat. The source of water for the ECCS pumps is automatically switched to the containment recirculation sump. Switchover from RWT to containment sump must occur before the RWT empties to prevent damage to the ECCS pumps and a loss of core cooling capability. For similar reasons, switchover must not occur before there is sufficient water in the containment sump to support pump suction. Furthermore, early switchover must not occur to ensure sufficient borated water is injected from the RWT to ensure the reactor remains shut down in the recirculation mode. An RWT Level - Low signal initiates the RAS.

BASES

APPLICABLE SAFETY ANALYSES (continued)

6. Auxiliary Feedwater Actuation Signal

An AFAS initiates feedwater flow to both steam generators if a low level is indicated in either steam generator, unless the generator is ruptured.

The AFAS maintains a steam generator heat sink during the following events:

- MSLB,
- FWLB,
- Inadvertent opening of a steam generator atmospheric dump valve, and
- Loss of feedwater.

A low steam generator water level signal will initiate auxiliary feed to the affected steam generator.

Secondary steam generator (SG) differential pressure (SG-A > SG-B) or (SG-B > SG-A) inhibits auxiliary feed to a generator identified as being ruptured. This input to the AFAS logic prevents loss of the intact generator while preventing feeding a ruptured generator during MSLBs and FWLBs. This prevents containment overpressurization during these events.

The ESFAS satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

The LCO requires that all components necessary to provide an ESFAS actuation be OPERABLE.

Actions allow maintenance bypass of individual channels. Plants are restricted to 48 hours in a maintenance bypass condition before either restoring the Function to four channel operation (two-out-of-four logic) or placing the channel in trip (one-out-of-three logic).

The Bases for the LCO on ESFAS automatic actuation Functions are addressed in the Bases for LCO 3.3.4. Those associated with the Manual Trip or Actuation Logic are addressed below.

BASES

LCO (continued)

1. Safety Injection Actuation Signal

    a. Manual Trip

        This LCO requires two channels of SIAS Manual Trip to be OPERABLE in MODES 1, 2, 3, and 4.

    b. Actuation Logic

        This LCO requires two channels of SIAS Actuation Logic to be OPERABLE in MODES 1, 2, 3, and 4.

        Failures in the actuation subsystems, including the manual bypass key switches, are Actuation Logic failures and are addressed in this LCO.

        Actuation Logic consists of all circuitry housed within the actuation subsystems, including the initiating relay contacts responsible for actuating the ESF equipment.

2. Containment Spray Actuation Signal

    CSAS is initiated either manually or automatically. At many plants it is also necessary to have an automatic or manual SIAS for a complete actuation. The SIAS opens the containment spray valves, whereas the CSAS actuates other required components. The SIAS requirement should always be satisfied on a legitimate CSAS, since the Containment Pressure - High signal used in the SIAS is the same setpoint used in the CSAS. The transmitters used to initiate CSAS are independent of those used in the SIAS to prevent inadvertent containment spray due to failures in two sensor channels.

    a. Manual Trip

        This LCO requires two channels of CSAS Manual Trip to be OPERABLE in MODES 1, 2, 3, and 4.

    b. Actuation Logic

        This LCO requires two channels of CSAS Actuation Logic to be OPERABLE in MODES 1, 2, 3, and 4.

        Actuation Logic consists of all circuitry housed within the actuation subsystems, including the initiating relay contacts responsible for actuating the ESF equipment.

BASES

LCO (continued)

3. Containment Isolation Actuation Signal

a. Manual Trip

This LCO requires two channels of CIAS Manual Trip to be OPERABLE in MODES 1, 2, 3, and 4.

b. Actuation Logic

This LCO requires two channels of Actuation Logic for CIAS to be OPERABLE in MODES 1, 2, 3, and 4.

Actuation Logic consists of all circuitry housed within the actuation subsystems, including the initiating relay contacts responsible for actuating the ESF equipment.

4. Main Steam Isolation Signal

a. Manual Trip

This LCO requires two channels per steam generator of the MSIS Manual Trip to be OPERABLE in MODES 1, 2, 3, and 4.

b. Actuation Logic

This LCO requires two channels of MSIS Actuation Logic to be OPERABLE in MODES 1, 2, 3, and 4.

Failures in the actuation subsystems, including the manual bypass key switches, are considered Actuation Logic failures and are addressed in the logic LCO.

5. Recirculation Actuation Signal

a. Manual Trip

This LCO requires two channels of RAS Manual Trip to be OPERABLE in MODES 1, 2, 3, and 4.

b. Actuation Logic

This LCO requires two channels of RAS Actuation Logic to be OPERABLE in MODES 1, 2, 3, and 4.

BASES

LCO (continued)

6. Auxiliary Feedwater Actuation Signal

A low level in either generator, as sensed by a two-out-of-four coincidence of four wide range sensors for each generator, will generate an auxiliary feedwater actuation signal (AFAS), which starts both trains of auxiliary feedwater (AFW) pumps and feeds both steam generators. The AFAS also monitors the secondary differential pressure in both steam generators and initiates an AFAS block signal to a ruptured generator if the pressure in that generator is lower than the other generator by the differential pressure setpoint.

a. Manual Trip

This LCO requires two channels of AFAS Manual Trip to be OPERABLE in MODES 1, 2, and 3.

b. Actuation Logic

This LCO requires two channels of AFAS Actuation Logic to be OPERABLE in MODES 1, 2, and 3.

Actuation Logic consists of all circuitry housed within the actuation subsystems, including the initiating relay contacts responsible for actuating the ESF equipment.

APPLICABILITY

All ESFAS Functions are required to be OPERABLE in MODES 1, 2, and 3. In MODES 1, 2, and 3, there is sufficient energy in the primary and secondary systems to warrant automatic ESF System responses to:

- Close the MSIVs to preclude a positive reactivity addition,
- Actuate AFW to preclude the loss of the steam generators as a heat sink (in the event the normal feedwater system is not available),
- Actuate ESF systems to prevent or limit the release of fission product radioactivity to the environment by isolating containment and limiting the containment pressure from exceeding the containment design pressure during a design basis LOCA or MSLB, and
- Actuate ESF systems to ensure sufficient borated inventory to permit adequate core cooling and reactivity control during a design basis LOCA or MSLB accident.

BASES

APPLICABILITY (continued)

In MODES 4, 5, and 6, automatic actuation of ESFAS Functions is not required, because adequate time is available for plant operators to evaluate plant conditions and respond by manually operating the ESF components if required. ESFAS Manual Trip capability is required for Functions other than AFAS in MODE 4 even though automatic actuation is not required. Because of the large number of components actuated on each ESFAS, actuation is simplified by the use of the Manual Trip push buttons. Manual Trip of AFAS is not required in MODE 4 because AFW or shutdown cooling will already be in operation in this MODE.

The ESFAS Actuation Logic must be OPERABLE in the same MODES as the Automatic and Manual Trips. In MODE 4, only the portion of the ESFAS logic responsible for the required Manual Trip must be OPERABLE.

In MODES 5 and 6, ESFAS initiated systems are either reconfigured or disabled for shutdown cooling operation. Accidents in these MODES are slow to develop and would be mitigated by manual operation of individual components.

ACTIONS

When the number of inoperable channels in a trip Function exceeds those specified in any related Condition associated with the same trip Function, then the plant is outside the safety analysis. Therefore, LCO 3.0.3 should be immediately entered, if applicable in the current MODE of operation.

A Note has been added to the ACTIONS to clarify the application of the Completion Time rules. The Conditions of this Specification may be entered independently for each Function in Table 3.3.5-1 in the LCO. Completion Times for the inoperable channel of a Function will be tracked separately.

A.1

Condition A applies to one AFAS Manual Trip or AFAS Actuation Logic channel inoperable. It is identical to Condition C for the other ESFAS Functions, except for the shutdown track imposed by Condition D.

The channel must be restored to OPERABLE status to restore redundancy of the AFAS Function. The 48 hour Completion Time is commensurate with the importance of avoiding the vulnerability of a single failure in the only remaining OPERABLE channel.

BASES

ACTIONS (continued)

B.1 and B.2

If two Manual Trip or Actuation Logic channels are inoperable or the Required Action and associated Completion Time of Condition A cannot be met, the reactor should be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 4 within [12] hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

C.1

Condition C applies to one Manual Trip or Actuation Logic channel inoperable for those ESFAS Functions that must be OPERABLE in MODES 1, 2, 3, and 4 (all Functions except AFAS). The shutdown track imposed by Condition D requires entry into MODE 5, where the LCO does not apply to the affected Functions.

The channel must be restored to OPERABLE status to restore redundancy of the affected Functions. The 48 hour Completion Time is commensurate with the importance of avoiding the vulnerability of a single failure in the only remaining OPERABLE channel.

D.1 and D.2

Condition D is entered when one or more Functions have two Manual Trip or Actuation Logic channels inoperable except AFAS or the Required Action and associated Completion Time of Condition C are not met. If Required Action C.1 cannot be met within the required Completion Time, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 5 within 36 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.3.5.1

A CHANNEL FUNCTIONAL TEST is performed every 92 days to ensure the entire channel will perform its intended function when needed. Sensor subsystem tests are addressed in LCO 3.3.4. This SR addresses Actuation Logic tests. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

Actuation Logic Tests

Actuation subsystem testing includes injecting one trip signal into each two-out-of-four logic subsystem in each ESFAS Function and using a bistable trip input to satisfy the trip logic. Initiation relays associated with the affected channel will then actuate the individual ESFAS components. Since each ESFAS Function employs subchannels of Actuation Logic, it is possible to actuate individual components without actuating an entire ESFAS Function.

Note 1 requires that Actuation Logic tests include operation of initiation relays. Note 2 allows deferred at power testing of certain relays to allow for the fact that operating certain relays during power operation could cause plant transients or equipment damage. Those initiation relays that cannot be tested at power must be tested in accordance with Note 2. These include [SIAS No. 5, SIAS No. 10, CIAS No. 5, and MSIS No. 1.]

These relays actuate the following components, which cannot be tested at power:

- RCP seal bleedoff isolation valves,
- Service water isolation valves,
- VCT discharge valves,
- Letdown stop valves,
- CCW to and from the RCPs,
- MSIVs and feedwater isolation valves, and
- Instrument air containment isolation valves.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The reasons that each of the above cannot be fully tested at power are stated in Reference 1.

These tests verify that the ESFAS is capable of performing its intended function, from bistable input through the actuated components.

The Frequency of [92] days is based on the reliability analysis presented in topical report CEN-327, "RPS/ESFAS Extended Test Interval Evaluation" (Ref. 2).

SR 3.3.5.2

A CHANNEL FUNCTIONAL TEST is performed on the manual ESFAS actuation circuitry, de-energizing relays and providing Manual Trip of the Function. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

This Surveillance verifies that the trip push buttons are capable of opening contacts in the Actuation Logic as designed, de-energizing the initiation relays and providing Manual Trip of the Function. The [18] month Frequency is based on the need to perform this Surveillance under the conditions that apply during a plant outage and the potential for an unplanned transient if the Surveillance were performed with the reactor at power. Operating experience has shown these components usually pass the Surveillance when performed at a Frequency of once every [18] months.

REFERENCES

1. FSAR, Section [7.3].

2. CEN-327, June 2, 1986, including Supplement 1, March 3, 1989.

B 3.3 INSTRUMENTATION

B 3.3.6 Diesel Generator (DG) - Loss of Voltage Start (LOVS) (Analog)

BASES

BACKGROUND

The DGs provide a source of emergency power when offsite power is either unavailable or insufficiently stable to allow safe plant operation. Undervoltage protection will generate a LOVS in the event a Loss of Voltage or Degraded Voltage condition occurs. There are two LOVS Functions for each 4.16 kV vital bus.

Four undervoltage relays with inverse time characteristics are provided on each 4.16 kV Class 1E instrument bus for the purpose of detecting a sustained undervoltage condition or a loss of bus voltage. The relays are combined in a two-out-of-four logic to generate a LOVS if the voltage is below 75% for a short time or below 90% for a long time. The LOVS initiated actions are described in Reference 1.

Trip Setpoints and Allowable Values

The trip setpoints and Allowable Values are based on the analytical limits presented in Reference 2. The selection of these trip setpoints is such that adequate protection is provided when all sensor and processing time delays are taken into account. To allow for calibration tolerances, instrumentation uncertainties, and instrument drift, Allowable Values specified in SR 3.3.6.3 are conservatively adjusted with respect to the analytical limits. A detailed description of the methodology used to calculate the trip setpoints, including their explicit uncertainties, is provided in Reference 3. The actual nominal trip setpoint is normally still more conservative than that required by the plant specific setpoint calculations. If the measured setpoint does not exceed the documented surveillance trip acceptance criteria, the undervoltage relay is considered OPERABLE.

Setpoints in accordance with the Allowable Values will ensure that the consequences of accidents will be acceptable, providing the plant is operated from within the LCOs at the onset of the accident and the equipment functions as designed.

BASES

BACKGROUND (continued)

The undervoltage protection scheme has been designed to protect the plant from spurious trips caused by the offsite power source. This is made possible by the inverse voltage time characteristics of the relays used. A complete loss of offsite power will result in approximately a 1 second delay in LOVS actuation. The DG starts and is available to accept loads within a 10 second time interval on the Engineered Safety Features Actuation System (ESFAS) or LOVS. Emergency power is established within the maximum time delay assumed for each event analyzed in the accident analysis (Ref. 2).

Since there are four protective channels in a two-out-of-four trip logic for each division of the 4.16 kV power supply, no single failure will cause or prevent protective system actuation. This arrangement meets IEEE Standard 279-1971 criteria (Ref. 4).

APPLICABLE SAFETY ANALYSES

The DG - LOVS is required for Engineered Safety Features (ESF) systems to function in any accident with a loss of offsite power. Its design basis is that of the ESFAS.

Accident analyses credit the loading of the DG based on a loss of offsite power during a loss of coolant accident. The actual DG start has historically been associated with the ESFAS actuation. The diesel loading has been included in the delay time associated with each safety system component requiring DG supplied power following a loss of offsite power. The analysis assumes a nonmechanistic DG loading, which does not explicitly account for each individual component of the loss of power detection and subsequent actions. This delay time includes contributions from the DG start, DG loading, and Safety Injection System component actuation. The response of the DG to a loss of power must be demonstrated to fall within this analysis response time when including the contributions of all portions of the delay.

The required channels of LOVS, in conjunction with the ESF systems powered from the DGs, provide plant protection in the event of any of the analyzed accidents discussed in Reference 2, in which a loss of offsite power is assumed. LOVS channels are required to meet the redundancy and testability requirements of GDC 21 in 10 CFR 50, Appendix A (Ref. 5).

The delay times assumed in the safety analysis for the ESF equipment include the [10] second DG start delay and the appropriate sequencing delay, if applicable. The response times for ESFAS actuated equipment include the appropriate DG loading and sequencing delay.

The DG - LOVS channels satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO

The LCO for the LOVS requires that four channels per bus of each LOVS instrumentation Function be OPERABLE in MODES 1, 2, 3, and 4 and when the associated DG is required to be OPERABLE by LCO 3.8.2, "AC Sources - Shutdown." The LOVS supports safety systems associated with the ESFAS. In MODES 5 and 6, the four channels must be OPERABLE whenever the associated DG is required to be OPERABLE to ensure that the automatic start of the DG is available when needed.

Actions allow maintenance (trip channel) bypass of individual channels. Plants are restricted to 48 hours in a trip channel bypass condition before either restoring the Function to four channel operation (two-out-of-four logic) or placing the channel in trip (one-out-of-three logic). At plants where adequate channel to channel independence has been demonstrated, specific exceptions have been approved by the NRC staff to permit one of the two-out-of-four channels to be bypassed for an extended period of time.

Loss of LOVS Function could result in the delay of safety system initiation when required. This could lead to unacceptable consequences during accidents. During the loss of offsite power, which is an anticipated operational occurrence, the DG powers the motor driven auxiliary feedwater pumps. Failure of these pumps to start would leave only the one turbine driven pump as well as an increased potential for a loss of decay heat removal through the secondary system.

Only Allowable Values are specified for each Function in the LCO. Nominal trip setpoints are specified in the plant specific setpoint calculations. The nominal setpoints are selected to ensure that the setpoint measured by CHANNEL FUNCTIONAL TESTS does not exceed the Allowable Value if the bistable is performing as required. Operation with a trip setpoint less conservative than the nominal trip setpoint, but within the Allowable Value, is acceptable, provided that operation and testing are consistent with the assumptions of the plant specific setpoint calculation. A channel is inoperable if its actual trip setpoint is not within its required Allowable Value.

[For this unit, the Bases for the Allowable Values and trip setpoints are as follows:]

BASES

APPLICABILITY

The DG - LOVS actuation Function is required in MODES 1, 2, 3, and 4 because ESF Functions are designed to provide protection in these MODES. Actuation in MODE 5 or 6 is required whenever the required DG must be OPERABLE, so that it can perform its function on a loss of power or degraded power to the vital bus.

ACTIONS

A LOVS channel is inoperable when it does not satisfy the OPERABILITY criteria for the channel's Function. The most common cause of channel inoperability is outright failure or drift of the bistable or process module sufficient to exceed the tolerance allowed by the plant specific setpoint analysis. Typically, the drift is found to be small and results in a delay of actuation rather than a total loss of function. Determination of setpoint drift is generally made during the performance of a CHANNEL FUNCTIONAL TEST when the instrument is set up for adjustment to bring it within specification. If the actual trip setpoint is not within the Allowable Value, the channel is inoperable and the appropriate Conditions must be entered.

In the event a channel's trip setpoint is found nonconservative with respect to the Allowable Value, or the channel is found inoperable, then all affected Functions provided by that channel must be declared inoperable and the LCO Condition entered. The required channels are specified on a per DG basis.

When the number of inoperable channels in a trip Function exceeds those specified in any related Condition associated with the same trip Function, then the plant is outside the safety analysis. Therefore, LCO 3.0.3 should be entered immediately if applicable in the current MODE of operation.

A Note has been added to the ACTIONS to clarify the application of Completion Time rules. The Conditions of this LCO may be entered independently for each Function. The Completion Time(s) of the inoperable channel(s)/train(s) of a Function will be tracked separately for each Function, starting from the time the Condition was entered for that Function.

A.1, A.2.1, and A.2.2

Condition A applies if one channel is inoperable for one or more Functions per DG bus.

If the channel cannot be restored to OPERABLE status, the affected channel should either be bypassed or tripped within 1 hour (Required Action A.1).

BASES

ACTIONS (continued)

Placing this channel in either Condition ensures that logic is in a known configuration. In trip, the LOVS Logic is one-out-of-three. In bypass, the LOVS Logic is two-out-of-three. The 1 hour Completion Time is sufficient to perform these Required Actions.

Once Required Action A.1 has been complied with, Required Action A.2.1 allows [48] hours to repair the inoperable channel for those plants that have not demonstrated sufficient channel to channel independence on this Function. If the channel cannot be restored to OPERABLE status, it must be tripped in accordance with Required Action A.2.2. The time allowed to repair or trip the channel is reasonable to repair the affected channel while ensuring that the risk involved in operating with the inoperable channel is acceptable. The [48] hour Completion Time is based upon operating experience, which has demonstrated that a random failure of a second channel is a rare event during any given [48] hour period.

<u>B.1, B.2.1, and B.2.2</u>

Condition B applies if two channels are inoperable for one or more Functions per DG.

If the channel cannot be restored to OPERABLE status within 1 hour, the Conditions and Required Actions for the associated DG made inoperable by DG - LOVS instrumentation are required to be entered. Alternatively, one affected channel is required to be bypassed and the other is tripped, in accordance with Required Action B.2.1. This places the Function in one-out-of-two logic. The 1 hour Completion Time is sufficient to perform the Required Actions.

Once Required Action B.2.1 has been complied with, Required Action B.2.2 allows [48] hours to repair the bypassed or inoperable channel.

After one channel is restored to OPERABLE status, the provisions of Condition A still apply to the remaining inoperable channel. Therefore, the channel that is still inoperable after completion of Required Action B.2.2 shall be placed in trip if more than [48] hours have elapsed since the initial channel failure.

BASES

ACTIONS (continued)

C.1

Condition C applies when more than two undervoltage or Degraded Voltage channels on a single bus are inoperable.

Required Action C.1 requires all but two channels to be restored to OPERABLE status within 1 hour. With more than two channels inoperable, the logic is not capable of providing a DG - LOVS signal for valid Loss of Voltage or Degraded Voltage conditions. The 1 hour Completion Time is reasonable to evaluate and take action to correct the degraded condition in an orderly manner and takes into account the low probability of an event requiring LOVS occurring during this interval.

D.1

Condition D applies if the Required Actions and associated Completion Times are not met.

Required Action D.1 ensures that Required Actions for the affected DG inoperabilities are initiated. Depending upon plant MODE, the actions specified in LCO 3.8.1, "AC Sources - Operating," or LCO 3.8.2 are required immediately.

SURVEILLANCE REQUIREMENTS

The following SRs apply to each DG - LOVS Function.

[SR 3.3.6.1

Performance of the CHANNEL CHECK once every 12 hours ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the indicated output of the potential transformers that feed the LOVS undervoltage relays. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value. Significant deviations between the two channels could be an indication of excessive drift in one of the channels or of something even more serious. CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying that the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

BASES

SURVEILLANCE REQUIREMENTS (continued)

Agreement criteria are determined by the plant staff, based on a combination of the channel instrument uncertainties, including indication and readability. If the channels are within the criteria, it is an indication that the channels are OPERABLE.]

[The Frequency, about once every shift, is based upon operating experience that demonstrates channel failure is rare. Since the probability of two random failures in redundant channels in any 12 hour period is extremely low, the CHANNEL CHECK minimizes the chance of loss of protective function due to failure of redundant channels. The CHANNEL CHECK supplements less formal, but more frequent, checks of channel OPERABILITY during normal operational use of the displays associated with the LCO required channels.]

<u>SR 3.3.6.2</u>

A CHANNEL FUNCTIONAL TEST is performed every [92] days to ensure that the entire channel will perform its intended function when needed. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

The Frequency of [92] days is based on plant operating experience with regard to channel OPERABILITY and drift, which demonstrates that failure of more than one channel of a given function in any [92] day Frequency is a rare event. Any setpoint adjustment shall be consistent with the assumptions of the current plant specific setpoint analysis.

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the surveillance interval extension analysis. The requirements for this review are outlined in Reference [6].

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.6.3

SR 3.3.6.3 is the performance of a CHANNEL CALIBRATION every 18 months. The CHANNEL CALIBRATION verifies the accuracy of each component within the instrument channel. This includes calibration of the undervoltage relays and demonstrates that the equipment falls within the specified operating characteristics defined by the manufacturer.

The Surveillance verifies that the channel responds to a measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drift between successive calibrations to ensure that the channel remains operational between successive tests. CHANNEL CALIBRATIONS must be performed consistent with the plant specific setpoint analysis.

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the surveillance interval extension analysis. The requirements for this review are outlined in Reference [6].

The setpoints, as well as the response to a Loss of Voltage and Degraded Voltage test, shall include a single point verification that the trip occurs within the required delay time as shown in Reference 1. The Frequency is based upon the assumption of an [18] month calibration interval for the determination of the magnitude of equipment drift in the setpoint analysis.

REFERENCES

1. FSAR, Section [8.3].
2. FSAR, Chapter [15].
3. "Plant Protection System Selection of Trip Setpoint Values."
4. IEEE Standard 279-1971.
5. 10 CFR 50, Appendix A, GDC 21.
6. [ ]

B 3.3 INSTRUMENTATION

B 3.3.7 Containment Purge Isolation Signal (CPIS) (Analog)

BASES

BACKGROUND

This LCO encompasses CPIS actuation, which is a plant specific instrumentation system that performs an actuation Function required for plant protection but is not otherwise included in LCO 3.3.5, "Engineered Safety Features Actuation System (ESFAS) Logic and Manual Trip," or LCO 3.3.6, "Diesel Generator (DG) - Loss of Voltage Start (LOVS)." This is a non-Nuclear Steam Supply System ESFAS Function that, because of differences in purpose, design, and operating requirements, is not included in LCOs 3.3.5 and 3.3.6. Details of this LCO are for illustration only. Individual plants shall include those Functions and LCO requirements applicable to them.

The CPIS provides protection from radioactive contamination in the containment in the event an irradiated fuel assembly should be severely damaged during handling.

The CPIS will detect any abnormal amounts of radioactive material in the containment and will initiate purge valve closure to limit the release of radioactivity to the environment. The containment purge supply and exhaust valves are closed on a CPIS when a high radiation level in containment is detected.

The CPIS includes two independent, redundant actuation subsystems. Where two isolation control valves are provided for a single containment penetration, each valve is controlled by a separate actuation subsystem. Where one valve is available, a single actuation subsystem initiates valve closure. One train also isolates the containment air exhaust fan, whereas the other train actuates the containment air supply fan. A list of actuated valves and an additional description of the CPIS are included in Reference 1. Both trains of CPIS are actuated on a two-out-of-four coincidence from the same four containment radiation sensor subsystems. Containment purge isolation also occurs on a Containment Isolation Actuation Signal (CIAS). The CIAS is addressed by LCO 3.3.4, "Engineered Safety Features Actuation System (ESFAS) Instrumentation."

BASES

BACKGROUND (continued)

Trip Setpoints and Allowable Values

Trip setpoints used in the bistables are based on the analytical limits stated in Reference 2. The selection of these trip setpoints is such that adequate protection is provided when all sensor and processing time delays are taken into account. To allow for calibration tolerances, instrumentation uncertainties, and instrument drift, Allowable Values specified in SR 3.3.7.2 are conservatively adjusted with respect to the analytical limits. A detailed description of the methodology used to calculate the trip setpoints, including their explicit uncertainties, is provided in "Plant Protection System Selection of Trip Setpoint Values" (Ref. 3). The actual nominal trip setpoint entered into the bistable is normally still more conservative than that specified by the Allowable Value to account for changes in random measurement errors detectable by a CHANNEL FUNCTIONAL TEST. One example of such a change in measurement error is drift during the surveillance interval. If the measured setpoint does not exceed the Allowable Value, the bistable is considered OPERABLE.

Setpoints in accordance with the Allowable Value will ensure that Safety Limits are not violated during anticipated operational occurrences (AOOs) and the consequences of Design Basis Accidents will be acceptable, providing the plant is operated from within the LCOs at the onset of the AOO or accident and the equipment functions as designed.

APPLICABLE SAFETY ANALYSES

The CPIS satisfies the requirements of Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

Only the Allowable Values are specified for each trip Function in the LCO. Operation with a trip setpoint less conservative than the nominal trip setpoint, but within its Allowable Value, is acceptable, provided that the difference between the nominal trip setpoint and the Allowable Value is equal to or greater than the drift allowance assumed for each trip in the transient and accident analyses.

Each Allowable Value specified is more conservative than the analytical limit assumed in the transient and accident analysis in order to account for instrument uncertainties appropriate to the trip Function. These uncertainties are defined in Reference 3. A channel is inoperable if its actual trip setpoint is not within its required Allowable Value.

BASES

LCO (continued)

The Bases for the LCO on the CPIS are discussed below for each Function:

a. Manual Trip

The LCO on Manual Trip backs up the automatic trips and ensures operators have the capability to rapidly initiate the CPIS Function if any parameter is trending toward its setpoint. At least one channel must be OPERABLE to be consistent with the requirements of LCO 3.9.3, "Containment Penetrations."

b. Containment Radiation - High

The LCO on the radiation channels requires that all four be OPERABLE.

[For this unit, the basis for the Containment Radiation - High setpoint is as follows:]

c. Actuation Logic

One train of Actuation Logic must be OPERABLE to be consistent with the requirements of LCO 3.9.3. If one fails, it must be restored to OPERABLE status.

APPLICABILITY

In MODE 5 or 6, the CPIS isolation of containment purge valves is not required to be OPERABLE. However, during movement of [recently] irradiated fuel [(i.e., fuel that has occupied part of a critical reactor core within the previous [X] days)], there is the possibility of a fuel handling accident requiring the CPIS on high radiation in containment. Accordingly, the CPIS must be OPERABLE during movement of [recently] irradiated fuel in containment.

In MODES 1, 2, 3, and 4, the containment purge valves are sealed closed.

BASES

ACTIONS

A CPIS channel is inoperable when it does not satisfy the OPERABILITY criteria for the channel's Function. The most common cause of channel inoperability is outright failure or drift of the bistable or process module sufficient to exceed the tolerance allowed by the plant specific setpoint analysis. Typically, the drift is not large and would result in a delay of actuation rather than a total loss of function. This determination is generally made during the performance of a CHANNEL FUNCTIONAL TEST when the process instrument is set up for adjustment to bring it within specification. If the actual trip setpoint is not within the Allowable Value in SR 3.3.7.2, the channel is inoperable and the appropriate Conditions must be entered.

In the event a channel's trip setpoint is found nonconservative with respect to the Allowable Value, or the sensor, instrument loop, signal processing electronics, or bistable is found inoperable, then all affected Functions provided by that channel should be declared inoperable and the LCO Condition entered for the particular protective function affected.

When the number of inoperable channels in a trip Function exceeds those specified in any related Condition associated with the same trip Function, then the plant is outside the safety analysis. Therefore, LCO 3.0.3 should be immediately entered if applicable in the current MODE of operation.

A.1 and A.2

Condition A applies to the failure of one Containment Radiation - High CPIS channel. The Required Action is to place the affected channel in the trip condition within 4 hours. The Completion Time accounts for the fact that three redundant channels monitoring containment radiation are still available to provide a single trip input to the CPIS logic to provide the automatic mitigation of a radiation release. Alternately, action must be taken to place the unit in a condition where the LCO does not apply. This does not preclude the movement of fuel to a safe position.

B.1 and B.2

Condition B applies to the failure of the required Manual Trip or automatic Actuation Logic train, to the failure of more than one radiation monitoring channel, or if the Required Action and associated Completion Time of Condition A are not met. Required Action B.1 is to place the containment purge and exhaust isolation valves in the closed position. The Required Action immediately performs the isolation Function of the CPIS. Required Action B.2 is to immediately enter the applicable Conditions and Required Actions for the affected isolation valves of LCO 3.9.3, "Containment Penetrations," that were made inoperable by the inoperable

BASES

ACTIONS (continued)

instrumentation of the CPIS LCO. The Required Action directs the operator to take actions that are appropriate for the containment isolation Function of the CPIS without initiating the containment air supply and exhaust fans. The Completion Time accounts for the fact that the automatic capability to isolate containment and initiate supply and exhaust fans on valid containment high radiation signals is degraded during conditions in which a fuel handling accident is possible and CPIS provides the only automatic mitigation of radiation release.

SURVEILLANCE REQUIREMENTS

SR 3.3.7.1

Performance of the CHANNEL CHECK once every 12 hours ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the parameter indicated on one channel to a similar parameter on other channels. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value.

Significant deviations between the two instrument channels could be an indication of excessive instrument drift in one of the channels or of something even more serious. CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

Agreement criteria are determined by the plant staff, based on a combination of the channel instrument uncertainties, including indication and readability. If a channel is outside the criteria, it may be an indication that the transmitter or the signal processing equipment has drifted outside its limits.

The Frequency, about once every shift, is based on operating experience that demonstrates the rarity of channel failure. Since the probability of two random failures in redundant channels in any 12 hour period is low, the CHANNEL CHECK minimizes the chance of loss of protective function due to failure of redundant channels. The CHANNEL CHECK supplements less formal, but more frequent, checks of channel OPERABILITY during normal operational use of the displays associated with the LCO required channels.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.7.2

A CHANNEL FUNCTIONAL TEST is performed on each containment radiation monitoring channel to ensure the entire channel will perform its intended function. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions. Any setpoint adjustment shall be consistent with the assumptions of the current plant specific setpoint analysis.

The Frequency of [92] days is based on plant operating experience with regard to channel OPERABILITY and drift, which demonstrates that failure of more than one channel of a given Function in any [92] day interval is a rare event.

SR 3.3.7.3

Proper operation of the initiation relays is verified by de-energizing these relays during the CHANNEL FUNCTIONAL TEST of the Actuation Logic every [31] days. This will actuate the Function, operating all associated equipment. Proper operation of the equipment actuated by each train is thus verified. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions. A Note indicates this Surveillance includes verification of operation for each initiation relay.

The Frequency of [31] days is based on plant operating experience with regard to channel OPERABILITY, which demonstrates that failure of more than one channel of a given Function in any [31] day interval is a rare event.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.7.4

CHANNEL CALIBRATION is a complete check of the instrument channel including the sensor. The Surveillance verifies that the channel responds to a measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drift between successive calibrations to ensure that the channel remains operational between successive tests. CHANNEL CALIBRATIONS must be performed consistent with the plant specific setpoint analysis.

The Frequency is based upon the assumption of an [18] month calibration interval for the determination of the magnitude of equipment drift in the setpoint analysis.

SR 3.3.7.5

Every [18] months, a CHANNEL FUNCTIONAL TEST is performed on the manual CPIS actuation circuitry. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

This Surveillance verifies that the trip push buttons are capable of opening contacts in the Actuation Logic as designed, de-energizing the initiation relays and providing Manual Trip of the Function. The [18] month Frequency is based on the need to perform this Surveillance under the conditions that apply during a plant outage and the potential for an unplanned transient if the Surveillance were performed with the reactor at power. Operating experience has shown these components usually pass the Surveillance when performed at a Frequency of once every 18 months.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.7.6

This Surveillance ensures that the train actuation response times are less than or equal to the maximum times assumed in the analyses. The 18 month Frequency is based upon plant operating experience, which shows random failures of instrumentation components causing serious response time degradation, but not channel failure, are infrequent occurrences. Testing of the final actuating devices, which make up the bulk of the response time, is included. Testing of the final actuating device in one channel is included in the testing of each actuation logic channel.

REFERENCES

1. FSAR, Section [6.2].

2. FSAR, Section [7.3].

3. "Plant Protection System Selection of Trip Setpoint Values."

B 3.3 INSTRUMENTATION

B 3.3.8 Control Room Isolation Signal (CRIS) (Analog)

BASES

BACKGROUND

This LCO encompasses CRIS actuation, which is a plant specific instrumentation channel that performs an actuation Function required for plant protection but is not otherwise included in LCO 3.3.5, "Engineered Safety Features Actuation System (ESFAS) Logic and Manual Trip," or LCO 3.3.6, "Diesel Generator (DG) - Loss of Voltage Start (LOVS)." This is a non-Nuclear Steam Supply System ESFAS Function that, because of differences in purpose, design, and operating requirements, is not included in LCO 3.3.5 and LCO 3.3.6. Details of this LCO are for illustration only. Individual plants shall include those Functions and LCO requirements that are applicable to them.

The CRIS terminates the normal supply of outside air to the control room and initiates actuation of the Emergency Radiation Protection System to minimize operator radiation exposure. The CRIS includes two independent, redundant subsystems, including actuation trains. Each train employs two separate sensors. One sensor detects gaseous activity. The other detects particulate and iodine activity. Since the two sensors detect different types of activity, they are not considered redundant to each other. However, since there are separate sensors in each train, the trains are redundant. If the bistable monitoring either sensor indicates an unsafe condition, that train will be actuated (one-out-of-two logic). The two trains actuate separate equipment. Actuating either train will perform the intended function. Control room isolation also occurs on a Safety Injection Actuation Signal (SIAS).

Trip Setpoints and Allowable Values

Trip setpoints used in the bistables are based on the analytical limits (Ref. 1). The selection of these trip setpoints is such that adequate protection is provided when all sensor and processing time delays are taken into account. To allow for calibration tolerances, instrumentation uncertainties, and instrument drift, Allowable Values specified in LCO 3.3.8 are conservatively adjusted with respect to the analytical limits. A detailed description of the methodology used to calculate the trip setpoints, including their explicit uncertainties, is provided in "Plant Protection System Selection of Trip Setpoint Values" (Ref. 2). The actual nominal trip setpoint entered into the bistable is normally still more

BASES

BACKGROUND (continued)

conservative than that specified by the Allowable Value to account for changes in random measurement errors detectable by a CHANNEL FUNCTIONAL TEST. One example of such a change in measurement error is drift during the surveillance interval. If the measured setpoint does not exceed the Allowable Value, the bistable is considered OPERABLE.

Setpoints in accordance with the Allowable Value will ensure that Safety Limits are not violated during anticipated operational occurrences (AOOs) and the consequences of Design Basis Accidents will be acceptable, providing the plant is operated from within the LCOs at the onset of the AOO or accident and the equipment functions as designed.

APPLICABLE SAFETY ANALYSES

The CRIS, in conjunction with the Control Room Emergency Air Cleanup System (CREACS), maintains the control room atmosphere within conditions suitable for prolonged occupancy throughout the duration of any one of the accidents discussed in Reference 1. The radiation exposure of control room personnel, through the duration of any one of the postulated accidents discussed in "Accident Analysis," FSAR, Chapter [15] (Ref. 1), does not exceed the limits set by 10 CFR 50, Appendix A, GDC 19 (Ref. 3).

The CRIS satisfies the requirements of Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

LCO 3.3.8 requires one channel of CRIS to be OPERABLE. The required channel consists of Actuation Logic, Manual Trip, and particulate/iodine and gaseous radiation monitors. The specific Allowable Values for the setpoints of the CRIS are listed in the SRs.

Only the Allowable Values are specified for each trip Function in the LCO. Operation with a trip setpoint less conservative than the nominal trip setpoint, but within its Allowable Value, is acceptable, provided that the difference between the nominal trip setpoint and the Allowable Value is equal to or greater than the drift allowance assumed for each trip in the transient and accident analyses.

Each Allowable Value specified is more conservative than the analytical limit assumed in the transient and accident analysis in order to account for instrument uncertainties appropriate to the trip Function. These uncertainties are defined in Reference 2. A channel is inoperable if its actual trip setpoint is not within its required Allowable Value.

BASES

LCO (continued)

The Bases for the LCO on the CRIS are discussed below for each Function:

a. Manual Trip

The LCO on Manual Trip backs up the automatic trips and ensures operators have the capability to rapidly initiate the CRIS Function if any parameter is trending toward its setpoint. One channel must be OPERABLE. This considers that the Manual Trip capability is a backup and that other means are available to actuate the redundant train if required, including manual SIAS.

b. Airborne Radiation

Both channels of Airborne Radiation detection in the required train are required to be OPERABLE to ensure the control room isolates on either high iodine and high particulate or gaseous concentration.

[For this unit, the basis for the Allowable Value is as follows:]

c. Actuation Logic

One train of Actuation Logic must be OPERABLE, since there are alternate means available to actuate the redundant train, including SIAS.

APPLICABILITY

The CRIS Functions must be OPERABLE in MODES 1, 2, 3, 4, [5, and 6] and during movement of [recently] irradiated fuel assemblies [(i.e., fuel that has occupied part of a critical reactor core within the previous [X] days)] to ensure a habitable environment for the control room operators.

----------------------------------REVIEWER'S NOTE-----------------------------------
For those plants that credit gas decay tank rupture accidents, the CRIS must also be OPERABLE in MODES 5 and 6.

ACTIONS

A CRIS channel is inoperable when it does not satisfy the OPERABILITY criteria for the channel's function. The most common cause of channel inoperability is outright failure or drift of the bistable or process module sufficient to exceed the tolerance allowed by the plant specific setpoint analysis. Typically, the drift is not large and would result in a delay of actuation rather than a total loss of function. This determination is

BASES

ACTIONS (continued)

generally made during the performance of a CHANNEL FUNCTIONAL TEST when the process instrument is set up for adjustment to bring it within specification. If the trip setpoint is not within the Allowable Value, the channel is inoperable and the appropriate Conditions must be entered.

A.1, B.1, B.2, C.1, C.2.1, and C.2.2

Conditions A and C have been modified by a Note, which specifies that CREACS be placed manually in the toxic gas protection mode if the automatic transfer to the toxic gas protection mode is inoperable. [At this unit, the basis for this Note is as follows:]

Conditions A, B, and C are applicable to manual and automatic actuation of the CREACS by CRIS. Condition A applies to the failure of the CRIS Manual Trip, Actuation Logic, and required particulate/iodine and required gaseous radiation monitor channels in MODE 1, 2, 3, or 4. Entry into this Condition requires action to either restore the failed channel(s) or manually perform the CRIS safety function (Required Action A.1). The Completion Time of 1 hour is sufficient to complete the Required Actions and accounts for the fact that CRIS supplements control room isolation by other Functions (e.g., SIAS) in MODES 1, 2, 3, and 4. If the channel cannot be restored to OPERABLE status, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours (Required Action B.1) and to MODE 5 within 36 hours (Required Action B.2). The Completion Times of 6 hours and 36 hours for reaching MODES 3 and 5 from MODE 1 are reasonable, based on operating experience and normal cooldown rates, for reaching the required MODE from full power conditions in an orderly manner and without challenging plant safety systems or operators.

Condition C applies to the failure of CRIS Manual Trip, Actuation Logic, and required particulate/iodine and required gaseous radiation monitor channels [in MODE 5 or 6] or when moving [recently] irradiated assemblies. The Required Actions are immediately taken to place one OPERABLE CREACS train in the emergency radiation protection mode or to suspend positive reactivity additions and movement of [recently] irradiated fuel assemblies. The Completion Time recognizes the fact that the radiation signals are the only Functions available to initiate control room isolation in the event of a fuel handling accident requiring control room isolation.

BASES

ACTIONS (continued)

Required Action [C.2.2] is modified by a Note to indicate that normal plant control operations that individually add limited positive reactivity (e.g., temperature or boron fluctuations associated with RCS inventory management or temperature control) are not precluded by this Action, provided they are accounted for in the calculated SDM.

SURVEILLANCE REQUIREMENTS

SR 3.3.8.1

Performance of the CHANNEL CHECK once every 12 hours ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the parameter indicated on one channel to a similar parameter on other channels. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value.

Significant deviations between the two instrument channels could be an indication of excessive instrument drift in one of the channels or of something even more serious. CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

Agreement criteria are determined by the plant staff based on a combination of the channel instrument uncertainties, including indication and readability. If a channel is outside the criteria, it may be an indication that the transmitter or the signal processing equipment has drifted outside its limit.

The Frequency, about once every shift, is based on operating experience that demonstrates the rarity of channel failure. Since the probability of two random failures in redundant channels in any 12 hour period is low, the CHANNEL CHECK minimizes the chance of loss of protective function due to failure of redundant channels. The CHANNEL CHECK supplements less formal, but more frequent, checks of channel OPERABILITY during normal operational use of the displays associated with the LCO required channels.

At this unit, the following administrative controls and design features (e.g., downscale alarms) immediately alert operations to loss of function in the nonredundant channels.

[At this unit, verification of sample system alignment and operation for gaseous, particulate, and iodine monitors is required as follows:]

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.8.2

A CHANNEL FUNCTIONAL TEST is performed on the required control room radiation monitoring channel to ensure the entire channel will perform its intended function. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions. Any setpoint adjustment shall be consistent with the assumptions of the current plant specific setpoint analysis.

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the frequency extension analysis. The requirements for this review are outlined in Reference [4].

The Frequency of [92] days is based on plant operating experience with regard to channel OPERABILITY and drift, which demonstrates that failure of more than one channel of a given Function in any [92] day interval is a rare event.

SR 3.3.8.3

Proper operation of the individual initiation relays is verified by de-energizing these relays during the CHANNEL FUNCTIONAL TEST of the Actuation Logic every [31] days. This will actuate the Function, operating all associated equipment. Proper operation of the equipment actuated by each train is thus verified. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

The Frequency of [31] days is based on plant operating experience with regard to channel OPERABILITY, which demonstrates that failure of more than one channel of a given Function in any [31] days interval is a rare event.

BASES

SURVEILLANCE REQUIREMENTS (continued)

Note 1 indicates this Surveillance includes verification of operation for each initiation relay.

Note 2 indicates that relays that cannot be tested at power are excepted from the Surveillance Requirement while at power. These relays must, however, be tested during each entry into MODE 5 exceeding 24 hours unless they have been tested within the previous 6 months.

SR 3.3.8.4

CHANNEL CALIBRATION is a complete check of the instrument channel including the sensor. The Surveillance verifies that the channel responds to a measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drift between successive calibrations to ensure that the channel remains operational between successive surveillances. CHANNEL CALIBRATIONS must be performed consistent with the plant specific setpoint analysis.

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the surveillance interval extension analysis. The requirements for this review are outlined in Reference [4].

The Frequency is based upon the assumption of an [18] month calibration interval for the determination of the magnitude of equipment drift in the setpoint analysis.

SR 3.3.8.5

Every [18] months, a CHANNEL FUNCTIONAL TEST is performed on the manual CRIS actuation circuitry. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

BASES

SURVEILLANCE REQUIREMENTS (continued)

This test verifies that the trip push buttons are capable of opening contacts in the Actuation Logic as designed, de-energizing the initiation relays and providing Manual Trip of the function. The [18] month Frequency is based on the need to perform this Surveillance under the conditions that apply during a plant outage and the potential for an unplanned transient if the Surveillance were performed with the reactor at power. Operating experience has shown these components usually pass the Surveillance when performed at a Frequency of once every [18] months.

[SR 3.3.8.6

This Surveillance ensures that the train actuation response times are less than the maximum times assumed in the analyses. The [18] month Frequency is based upon plant operating experience, which shows that random failures of instrumentation components causing serious response time degradation, but not channel failure, are infrequent occurrences. Testing of the final actuating devices, which make up the bulk of the response time, is included in the Surveillance testing.]

REFERENCES

1. FSAR, Chapter [15].
2. "Plant Protection System Selection of Trip Setpoint Values."
3. 10 CFR 50, Appendix A, GDC 19.
4. [ ].

B 3.3 INSTRUMENTATION

B 3.3.9 Chemical and Volume Control System (CVCS) Isolation Signal (Analog)

BASES

BACKGROUND

This LCO encompasses Chemical and Volume Control System (CVCS) Isolation Signal actuation. This is a plant specific instrumentation channel that performs an actuation Function required for plant protection and is not otherwise included in LCO 3.3.5, "Engineered Safety Features Actuation System (ESFAS) Logic and Manual Trip," or LCO 3.3.6, "Diesel Generator (DG) - Loss of Voltage Start (LOVS)." This is a non-Nuclear Steam Supply System ESFAS Function that, because of differences in purpose, design, and operating requirements, is not included in LCOs 3.3.5 and 3.3.6. Details of this LCO are for illustration only. Individual plants shall include those Functions and LCO requirements that are applicable to them.

The CVCS Isolation Signal provides protection from radioactive contamination, as well as personnel and equipment protection in the event of a letdown line rupture outside containment.

Each of the two actuation subsystems will isolate a separate letdown isolation valve in response to a high pressure condition in either the West Penetration Room or Letdown Heat Exchanger Room. Two pressure detectors in each of these rooms feed the four sensor subsystems. On a two-out-of-four coincidence, both actuation subsystems will actuate.

<u>Trip Setpoints and Allowable Values</u>

Trip setpoints used in the bistables are based on the analytical limits stated in Reference 1. The selection of these trip setpoints is such that adequate protection is provided when all sensor and processing time delays are taken into account. To allow for calibration tolerances, instrumentation uncertainties, and instrument drift, Allowable Values specified in SR 3.3.9.2 are conservatively adjusted with respect to the analytical limits. A detailed description of the methodology used to calculate the trip setpoints, including their explicit uncertainties, is provided in "Plant Protection System Selection of Trip Setpoint Values" (Ref. 2). The actual nominal trip setpoint entered into the bistable is normally still more conservative than that specified by the Allowable Value to account for changes in random measurement errors detectable by a CHANNEL FUNCTIONAL TEST. One example of such a change in measurement error is drift during the interval. If the measured setpoint does not exceed the Allowable Value, the bistable is considered OPERABLE.

BASES

BACKGROUND (continued)

Setpoints in accordance with the Allowable Value will ensure that Safety Limits are not violated during anticipated operational occurrences (AOOs) and the consequences of Design Basis Accidents will be acceptable, providing the plant is operated from within the LCOs at the onset of the AOO or accident and the equipment functions as designed.

APPLICABLE SAFETY ANALYSES

The CVCS Isolation Signal is redundant to the Safety Injection Actuation Signal for letdown line breaks outside containment. In addition, an excess flow check valve is located in containment just downstream of the regenerative heat exchanger, which isolates letdown when flow exceeds 200 gpm.

[At this unit, the provision of two sensors in each room in a two-out-of-four logic configuration satisfies the single failure criterion as follows:]

The CVCS satisfies the requirements of Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

Only the Allowable Values are specified for each trip Function in the LCO. Operation with a trip setpoint less conservative than the nominal trip setpoint, but within its Allowable Value, is acceptable, provided that the difference between the nominal trip setpoint and the Allowable Value is equal to or greater than the drift allowance assumed for each trip in the transient and accident analyses.

Each Allowable Value specified is more conservative than the analytical limit assumed in the transient and accident analysis, in order to account for instrument uncertainties appropriate to the trip Function. These uncertainties are defined in the "Plant Protection System Selection of Trip Setpoint Values" (Ref. 2).

CVCS isolation consists of closing the appropriate valve. This is undesirable at power, since letdown isolation will result. The absence of letdown flow will significantly decrease the charging flow temperature due to the absence of the regenerative heat exchanger preheating, causing unnecessary thermal stress to the charging nozzle. Therefore, the preferred action is to restore the valve function to OPERABLE status.

Four channels of West Penetration Room and Letdown Heat Exchanger Room pressure sensing and two Actuation Logic channels are required to be OPERABLE.

[For this unit, the Bases for the Allowable Values are as follows:]

[For this unit, the Bases for the LCO requirement are as follows:]

BASES

APPLICABILITY

The CVCS Isolation Signal must be OPERABLE in MODES 1, 2, 3, and 4, since the possibility of a loss of coolant accident is greatest in these MODES. In MODE 5 or 6, the probability is greatly diminished, and there is time to manually isolate CVCS.

ACTIONS

A CVCS isolation channel is inoperable when it does not satisfy the OPERABILITY criteria for the channel's Function. The most common cause of channel inoperability is outright failure or drift of the bistable or process module sufficient to exceed the tolerance allowed by the plant specific setpoint analysis. Typically, the drift is not large and would result in a delay of actuation rather than a total loss of function. This determination is generally made during the performance of a CHANNEL FUNCTIONAL TEST, when the process instrument is set up for adjustment to bring it within specification. If the trip setpoint is not consistent with the Allowable Value in SR 3.3.9.2, the channel must be declared inoperable immediately and the appropriate Conditions must be entered.

In the event a channel's trip setpoint is found nonconservative with respect to the Allowable Value, or the sensor, instrument loop, signal processing electronics, or bistable is found inoperable, then all affected Functions provided by that channel should be declared inoperable and the LCO Condition entered for the particular protection Function affected.

When the number of inoperable channels in a trip Function exceeds those specified in any related Condition associated with the same trip Function, then the plant is outside the safety analysis. Therefore, LCO 3.0.3 should be immediately entered if applicable in the current MODE of operation.

<u>A.1</u>

Condition A applies to the failure of one CVCS Actuation Logic channel associated with the CVCS Isolation Signal. Required Action A.1 requires restoration of the inoperable channel to restore redundancy of the affected Function. The Completion Time of 48 hours is consistent with the Completion Time of other ESFAS Functions and should be adequate for most repairs, while minimizing the risk of operating with an inoperable channel.

BASES

ACTIONS (continued)

B.1, B.2.1, and B.2.2

Condition B applies if one of the four CVCS instrument channels is inoperable. The Required Actions are identical to those of ESFAS Functions employing four redundant sensors specified in LCO 3.3.4, "Engineered Safety Features Actuation System (ESFAS) Instrumentation." The channel must be placed in bypass or trip if it cannot be repaired within 1 hour (Required Action B.1). The provision of four trip channels allows one channel to be bypassed (removed from service) during operations, placing the ESFAS in two-out-of-three coincidence logic. Placing the channel in bypass is preferred, since the CVCS isolation Function will be in two-out-of-three logic. This will avoid possible inadvertent CVCS isolation if an additional channel fails. The 1 hour Completion Time to bypass or trip the channel is sufficient time to perform the Required Actions.

Once the Required Action to trip or bypass the channel has been complied with, Required Action B.2.1 and Required Action B.2.2 provide for restoring the channel to OPERABLE status or placing it in trip within 48 hours. Required Action B.2.1 restores the full capability of the Function. Required Action B.2.2 places the Function in a one-out-of-three configuration. In this configuration, common cause failure of dependent channels cannot prevent CVCS isolation actuation. The Completion Time provides the operator with time to take appropriate actions and still ensures that any risk involved in operating with a failed channel is acceptable. It is improbable that a failure of a second channel will occur during any given 48 hour period.

C.1 and C.2

Condition C applies if two of the four CVCS West Penetration Room/Letdown Heat Exchanger Room Pressure - High channels are inoperable. The Required Actions are identical to those for other ESFAS Functions employing four redundant sensors in LCO 3.3.4.

Restoring at least one channel to OPERABLE status is the preferred Required Action. If this cannot be accomplished, one channel should be placed in bypass and the other channel in trip. The allowed Completion Time of 1 hour is sufficient time to perform the Required Actions.

BASES

ACTIONS (continued)

Once the Required Action to trip or bypass the channel has been complied with, Required Action C.2 provides for restoring one channel to OPERABLE status within 48 hours. The justification of the 48 hour Completion Time is the same as for Condition B.

After one channel is restored to OPERABLE status, the provisions of Condition C still apply to the remaining inoperable channel.

D.1 and D.2

Condition D specifies the shutdown track to be followed if two Actuation Logic channels are inoperable or if the Required Actions and associated Completion Times of Condition A, B, or C are not met. If two Actuation Logic channels are inoperable or the Required Actions cannot be met within the required Completion Time, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 5 within 36 hours. The Completion Times are reasonable, based on operating experience, to reach the required MODE from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.3.9.1

Performance of the CHANNEL CHECK on each CVCS isolation pressure indicating channel once every 12 hours ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the parameter indicated on one channel to a similar parameter on other channels. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value.

Significant deviations between the two instrument channels could be an indication of excessive instrument drift in one of the channels or of something even more serious. CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

Agreement criteria are determined by the plant staff based on a combination of the channel instrument uncertainties, including indication and readability. If a channel is outside the criteria, it may be an indication that the transmitter or the signal processing equipment has drifted outside its limit.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The Frequency, about once every shift, is based on operating experience that demonstrates the rarity of channel failure. Since the probability of two random failures in redundant channels in any 12 hour period is low, the CHANNEL CHECK minimizes the chance of loss of protective function due to failure of redundant channels. The CHANNEL CHECK supplements less formal, but more frequent, checks of channel OPERABILITY during normal operational use of the displays associated with the LCO required channels.

SR 3.3.9.2

A CHANNEL FUNCTIONAL TEST is performed on each channel to ensure the entire channel will perform its intended function. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions. Any setpoint adjustment shall be consistent with the assumptions of the current plant specific setpoint analysis.

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the surveillance interval extension analysis. The requirements for this review are outlined in Reference [3].

The Frequency of 31 days is based on plant operating experience with regard to channel OPERABILITY and drift, which demonstrates that failure of more than one channel of a given Function in any 31 day interval is a rare event.
Proper operation of the individual subgroup relays is verified by de-energizing these relays during the CHANNEL FUNCTIONAL TEST of the Actuation Logic every 31 days. This will actuate the Function, operating all associated equipment. Proper operation of the equipment actuated by each train is thus verified. Note 1 indicates this test includes verification of operation for each initiation relay. [At this unit, the verification is conducted as follows:]

Note 2 indicates that relays that cannot be tested at power are excepted from the SR while at power. These relays must, however, be tested during each entry into MODE 5 exceeding 24 hours unless they have been tested within the previous 6 months.

BASES

SURVEILLANCE REQUIREMENTS (continued)

[At this unit, the basis for this test exception is as follows:]

[At this unit, the following relays excepted by this Note are:]

SR 3.3.9.3

CHANNEL CALIBRATION is a complete check of the instrument channel including the sensor. The Surveillance verifies that the channel responds to a measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drift between successive calibrations to ensure that the channel remains operational between successive tests. CHANNEL CALIBRATIONS must be performed consistent with the plant specific setpoint analysis.

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the surveillance interval extension analysis. The requirements for this review are outlined in Reference [3].

Radiation detectors may be removed and calibrated in a laboratory, calibrated in place using a transfer source or replaced with an equivalent laboratory calibrated unit.

The Frequency is based upon the assumptions of an 18 month calibration interval for the determination of the magnitude of equipment drift in the setpoint analysis and includes operating experience as well as consistency with an 18 month fuel cycle.

REFERENCES

1. FSAR, Section [7.3].

2. "Plant Protection System Selection of Trip Setpoint Values."

3. [ ].

B 3.3 INSTRUMENTATION

B 3.3.10 Shield Building Filtration Actuation Signal (SBFAS) (Analog)

BASES

BACKGROUND	This LCO encompasses the SBFAS, which is a plant specific instrumentation system that performs an actuation Function required for plant protection but is not otherwise included in LCO 3.3.5, "Engineered Safety Features Actuation System (ESFAS) Logic and Manual Trip," or LCO 3.3.6, "Diesel Generator (DG) - Loss of Voltage Start (LOVS)." This is a non-Nuclear Steam Supply System ESFAS Function that, because of differences in purpose, design, and operating requirements, is not included in LCOs 3.3.5 and 3.3.6. Details of this LCO are for illustration only. Individual plants shall include those Functions and LCO requirements that are applicable to them.
APPLICABLE SAFETY ANALYSES	The SBFAS is required to filter the air space between the containment and shield building during a loss of coolant accident (LOCA), as discussed in FSAR, Chapter 15 (Ref. 1). The SBFAS satisfies the requirements of Criterion 3 of 10 CFR 50.36(c)(2)(ii).
LCO	The LCO on equipment OPERABILITY ensures that the SBFAS will perform as required when called upon. The LCO requires two channels of SBFAS automatic and Manual Trip to be OPERABLE. Two channels are necessary to ensure the required redundancy should one channel become inoperable.
APPLICABILITY	The SBFAS must be OPERABLE in MODES 1, 2, 3, and 4, since the possibility of a LOCA is greatest in these MODES. In MODE 5 or 6 the probability of a LOCA is greatly diminished, and there is ample time to respond manually to a LOCA event.
ACTIONS	When the number of inoperable channels in a trip Function exceeds those specified in the Conditions associated with the same trip Function, then the plant is outside the safety analysis. Therefore, LCO 3.0.3 should be immediately entered if applicable in the current MODE of operation.

BASES

ACTIONS (continued)

A.1

Condition A applies to the failure of one SBFAS Manual Trip channel or of one Actuation Logic associated with the Chemical and Volume Control System Isolation Signal or SBFAS. Required Action A.1 requires restoration of the inoperable channel to restore redundancy of the affected Function. The Completion Time of 48 hours is consistent with the Completion Time of other ESFAS Functions employing similar logic and should be adequate for most repairs while minimizing the risk of operating with an inoperable channel for a manually actuated Function.

B.1 and B.2

Condition B specifies the shutdown track to be followed if the Required Action and associated Completion Time of Condition A are not met. If Required Action A.1 cannot be met within the required Completion Time, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 5 within 36 hours. The Completion Times are reasonable, based on operating experience, to reach the required MODE from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.3.10.1

The SBFAS can be initiated either on a Safety Injection Actuation Signal (SIAS) or manually. This Surveillance is a restatement of SR 3.3.5.1 on the SIAS Function. Performing SR 3.3.5.1 satisfies this Surveillance. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions. The Frequency is the same as that for SR 3.3.5.1.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.10.2

Every [18] months, a CHANNEL FUNCTIONAL TEST is performed on the manual SBFAS actuation circuitry. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

This Surveillance verifies that the trip push buttons are capable of opening contacts in the Actuation Logic as designed, de-energizing the initiation relays and providing Manual Trip of the Function. The 18 month Frequency is based on the need to perform this Surveillance under the conditions that apply during a plant outage and the potential for an unplanned transient if the Surveillance were performed with the reactor at power. Operating experience has shown these components usually pass the Surveillance when performed at a Frequency of once every [18] months.

REFERENCES

1. FSAR, Chapter [15].

B 3.3 INSTRUMENTATION

B 3.3.11 Post Accident Monitoring (PAM) Instrumentation (Analog)

BASES

BACKGROUND

The primary purpose of the post accident monitoring (PAM) instrumentation is to display plant variables that provide information required by the control room operators during accident situations. This information provides the necessary support for the operator to take the manual actions, for which no automatic control is provided, that are required for safety systems to accomplish their safety Functions for Design Basis Events.

The OPERABILITY of the PAM instrumentation ensures that there is sufficient information available on selected plant parameters to monitor and assess plant status and behavior following an accident.

The availability of PAM instrumentation is important so that responses to corrective actions can be observed and the need for, and magnitude of, further actions can be determined. These essential instruments are identified by plant specific documents (Ref. 1) addressing the recommendations of Regulatory Guide 1.97 (Ref. 2), as required by Supplement 1 to NUREG-0737, "TMI Action Items" (Ref. 3).

Type A variables are included in this LCO because they provide the primary information required to permit the control room operator to take specific manually controlled actions, for which no automatic control is provided, that are required for safety systems to accomplish their safety functions for Design Basis Accidents (DBAs). Because the list of Type A variables differs widely between plants, Table 3.3.11-1, in the accompanying LCO, contains no examples of Type A variables, except for those that may also be Category I.

Category I variables are the key variables deemed risk significant because they are needed to:

- Determine whether other systems important to safety are performing their intended functions,
- Provide information to the operators that will enable them to determine the potential for causing a gross breach of the barriers to radioactivity release, and
- Provide information regarding the release of radioactive materials to allow for early indication of the need to initiate action necessary to protect the public and for an estimate of the magnitude of any impending threat.

BASES

BACKGROUND (continued)

These key variables are identified by plant specific Regulatory Guide 1.97 analyses (Ref. 1). These analyses identified the plant specific Type A and Category I variables and provided justification for deviating from the NRC proposed list of Category I variables.

----------------------------------REVIEWER'S NOTE----------------------------------
Table 3.3.11-1, in the accompanying LCO, provides a list of variables typical of those identified by plant specific Regulatory Guide 1.97 analyses. Table 3.3.11-1 in the plant specific Technical Specifications shall list all Type A and Category I variables identified by plant specific Regulatory Guide 1.97 analyses, as amended by NRC's Safety Evaluation Report (SER) (Ref. 4). The specific instrument Functions listed in Table 3.3.11-1 are discussed in the LCO Bases.

APPLICABLE SAFETY ANALYSES

The PAM instrumentation ensures the OPERABILITY of Regulatory Guide 1.97 Type A variables, so that the control room operating staff can:

- Perform the diagnosis specified in the emergency operating procedures. These variables are restricted to preplanned actions for the primary success path of DBAs and
- Take the specified, preplanned, manually controlled actions, for which no automatic control is provided, that are required for safety systems to accomplish their safety functions.

The PAM instrumentation also ensures OPERABILITY of Category I, non-Type A variables. This ensures the control room operating staff can:

- Determine whether systems important to safety are performing their intended functions,
- Determine the potential for causing a gross breach of the barriers to radioactivity release,
- Determine if a gross breach of a barrier has occurred, and
- Initiate action necessary to protect the public as well as to obtain an estimate of the magnitude of any impending threat.

BASES

APPLICABLE SAFETY ANALYSES (continued)

PAM instrumentation that satisfies the definition of Type A in Regulatory Guide 1.97 meets Criterion 3 of 10 CFR 50.36(c)(2)(ii).

Category I, non-Type A PAM instruments are retained in the Specification because they are intended to assist operators in minimizing the consequences of accidents. Therefore, these Category I variables are important in reducing public risk.

LCO

LCO 3.3.11 requires two OPERABLE channels for all but one Function to ensure no single failure prevents the operators from being presented with the information necessary to determine the status of the plant and to bring the plant to, and maintain it in, a safe condition following that accident.

Furthermore, provision of two channels allows a CHANNEL CHECK during the post accident phase to confirm the validity of displayed information.

[More than two channels may be required at some units if the Regulatory Guide 1.97 analysis determined that failure of one PAM channel results in information ambiguity (that is, the redundant displays disagree) that could lead operators to defeat or to fail to accomplish a required safety function.]

The exception to the two channel requirement is Penetration Flow Path Containment Isolation Valve Position. In this case, the important information is the status of the containment penetrations. The LCO requires one position indicator for each active containment isolation valve. This is sufficient to redundantly verify the isolation status of each isolable penetration either via indicated status of the active valve and prior knowledge of the passive valve or via system boundary status. If a normally active containment isolation valve is known to be closed and deactivated, position indication is not needed to determine status. Therefore, the position indication for valves in this state is not required to be OPERABLE.

Listed below are discussions of the specified instrument Functions listed in Table 3.3.11-1. These discussions are intended as examples of what should be provided for each Function when the plant specific list is prepared.

BASES

LCO (continued)

1. [Logarithmic] Neutron Flux[

Logarithmic] Neutron Flux indication is provided to verify reactor shutdown.

[At this unit, the [Logarithmic] Neutron Flux PAM channels consist of the following:]

2, 3. Reactor Coolant System (RCS) Hot and Cold Leg Temperature

RCS Hot and Cold Leg Temperatures are Category I variables provided for verification of core cooling and long term surveillance.

Reactor outlet temperature inputs to the PAM are provided by two fast response resistance elements and associated transmitters in each loop. The channels provide indication over a range of 32°F to 700°F.

4. Reactor Coolant System Pressure (wide range)

RCS wide range pressure is a Category I variable provided for verification of core cooling and RCS integrity long term surveillance.

Wide range RCS loop pressure is measured by pressure transmitters with a span of 0 psig to 3000 psig. The pressure transmitters are located outside the containment. Redundant monitoring capability is provided by two trains of instrumentation. Control room indications are provided through the inadequate core cooling (ICC) plasma display. The ICC plasma display is the primary indication used by the operator during an accident. Therefore, the PAM instrumentation LCO deals specifically with this portion of the instrument channel.

In some plants, RCS pressure is a Type A variable because the operator uses this indication to monitor the cooldown of the RCS following a steam generator tube rupture or small break loss of coolant accident (LOCA). Operator actions to maintain a controlled cooldown, such as adjusting steam generator pressure or level, would use this indication. Furthermore, RCS pressure is one factor that may be used in decisions to terminate reactor coolant pump operation.

BASES

LCO (continued)

5. Reactor Vessel Water Level

Reactor Vessel Water Level is provided for verification and long term surveillance of core cooling.

The Reactor Vessel Water Level monitoring system provides a direct measurement of the collapsed liquid level above the fuel alignment plate. The collapsed level represents the amount of liquid mass that is in the reactor vessel above the core. Measurement of the collapsed water level is selected because it is a direct indication of the water inventory. The collapsed level is obtained over the same temperature and pressure range as the saturation measurements, thereby encompassing all operating and accident conditions where it must function. Also, it functions during the recovery interval. Therefore, it is designed to survive the high steam temperature that may occur during the preceding core recovery interval.

The level range extends from the top of the vessel down to the top of the fuel alignment plate. The response time is short enough to track the level during small break LOCA events. The resolution is sufficient to show the initial level drop, the key locations near the hot leg elevation, and the lowest levels just above the alignment plate. This provides the operator with adequate indication to track the progression of the accident and to detect the consequences of its mitigating actions or the functionality of automatic equipment.

6. Containment Sump Water Level (wide range)

Containment Sump Water Level is provided for verification and long term surveillance of RCS integrity.

[For this unit, Containment Sump Water Level instrumentation consists of the following:]

7. Containment Pressure (wide range)

Containment Pressure is provided for verification of RCS and containment OPERABILITY.

[For this unit, Containment Pressure instrumentation consists of the following:]

BASES

LCO (continued)

8. Penetration Flow Path Containment Isolation Valve Position

Penetration Flow Path Containment Isolation Valve (CIV) Position is provided for verification of containment OPERABILITY.

CIV position is provided for verification of containment integrity. In the case of CIV position, the important information is the isolation status of the containment penetration. The LCO requires one channel of valve position indication in the control room to be OPERABLE for each active CIV in a containment penetration flow path, i.e., two total channels of CIV position indication for a penetration flow path with two active valves. For containment penetrations with only one active CIV having control room indication, Note (b) requires a single channel of valve position indication to be OPERABLE. This is sufficient to redundantly verify the isolation status of each isolable penetration via indicated status of the active valve, as applicable, and prior knowledge of passive valve or system boundary status. If a penetration flow path is isolated, position indication for the CIV(s) in the associated penetration flow path is not needed to determine status. Therefore, the position indication for valves in an isolated penetration flow path is not required to be OPERABLE. Each penetration is treated separately and each penetration flow path is considered a separate function. Therefore, separate Condition entry is allowed for each inoperable penetration flow path.

[For this unit, the CIV position PAM instrumentation consists of the following:]

9. Containment Area Radiation (high range)

Containment Area Radiation is provided to monitor for the potential of significant radiation releases and to provide release assessment for use by operators in determining the need to invoke site emergency plans.

[For this unit, Containment Area Radiation instrumentation consists of the following:]

BASES

LCO (continued)

10. Pressurizer Level

Pressurizer Level is used to determine whether to terminate safety injection (SI), if still in progress, or to reinitiate SI if it has been stopped. Knowledge of pressurizer water level is also used to verify the plant conditions necessary to establish natural circulation in the RCS and to verify that the plant is maintained in a safe shutdown condition.

[For this unit, Pressurizer Level instrumentation consists of the following:]

11. Steam Generator Water Level

Steam Generator Water Level is provided to monitor operation of decay heat removal via the steam generators. The Category I indication of steam generator level is the extended startup range level instrumentation. The extended startup range level covers a span of 6 inches to 394 inches above the lower tubesheet. The measured differential pressure is displayed in inches of water at 68°F. Temperature compensation of this indication is performed manually by the operator. Redundant monitoring capability is provided by two trains of instrumentation. The uncompensated level signal is input to the plant computer, a control room indicator, and the [Auxiliary Feedwater (AFW)] Control System.

At some plants, operator action is based on the control room indication of Steam Generator Water Level. The RCS response during a design basis small break LOCA is dependent on the break size. For a certain range of break sizes, the boiler condenser mode of heat transfer is necessary to remove decay heat. At these plants, extended startup range level is a Type A variable because the

operator must manually raise and control the steam generator level to establish boiler condenser heat transfer. Operator action is initiated on a loss of subcooled margin. Feedwater flow is increased until the indicated extended startup range level reaches the boiler condenser setpoint.

BASES

LCO (continued)

12. Condensate Storage Tank (CST) Level

CST Level is provided to ensure water supply for [AFW]. The CST provides the ensured safety grade water supply for the [AFW] System. The CST consists of two identical tanks connected by a common outlet header. Inventory is monitored by a 0 to 144 inch level indication for each tank. CST Level is displayed on a control room indicator, strip chart recorder, and plant computer. In addition, a control room annunciator alarms on low level.

At some plants, CST Level is considered a Type A variable because the control room meter and annunciator are considered the primary indication used by the operator. The DBAs that require [AFW] are the loss of electric power, steam line break (SLB), and small break LOCA. The CST is the initial source of water for the [AFW] System. However, as the CST is depleted, manual operator action is necessary to replenish the CST or align suction to the [AFW] pumps from the hotwell.

13, 14, 15, 16. Core Exit Temperature

Core Exit Temperature is provided for verification and long term surveillance of core cooling.

An evaluation was made of the minimum number of valid core exit thermocouples necessary for inadequate core cooling detection. The evaluation determined the reduced complement of core exit thermocouples necessary to detect initial core uncovery and trend the ensuing core heatup. The evaluations account for core nonuniformities including incore effects of the radial decay power distribution and excore effects of condensate runback in the hot legs and nonuniform inlet temperatures. Based on these evaluations, adequate or inadequate core cooling detection is ensured with two valid core exit thermocouples per quadrant.

The design of the Incore Instrumentation System includes a Type K (chromel alumel) thermocouple within each of the 56 incore instrument detector assemblies.

BASES

LCO (continued)

The junction of each thermocouple is located a few inches above the fuel assembly, inside a structure that supports and shields the incore instrument detector assembly string from flow forces in the outlet plenum region. These core exit thermocouples monitor the temperature of the reactor coolant as it exits the fuel assemblies.

The core exit thermocouples have a usable temperature range from 32°F to 2300°F, although accuracy is reduced at temperatures above 1800°F.

17. [Auxiliary Feedwater (AFW)] Flow

[AFW] Flow is provided to monitor operation of decay heat removal via the steam generators.

The [AFW] Flow to each steam generator is determined from a differential pressure measurement calibrated to a span of 0 gpm to 1200 gpm. Redundant monitoring capability is provided by two independent trains of instrumentation for each steam generator. Each differential pressure transmitter provides an input to a control room indicator and the plant computer. Since the primary indication used by the operator during an accident is the control room indicator, the PAM instrumentation Specification deals specifically with this portion of the instrument channel.

At some plants [AFW] Flow is a Type A variable because operator action is required to throttle flow during an SLB accident in order to prevent the [AFW] pumps from operating in runout conditions. [AFW] Flow is also used by the operator to verify that the [AFW] System is delivering the correct flow to each steam generator. However, the primary indication used by the operator to ensure an adequate inventory is steam generator level.

Two channels are required to be OPERABLE for all but one Function. Two OPERABLE channels ensure that no single failure, within either the PAM instrumentation or its auxiliary supporting features or power sources (concurrent with the failures that are a condition of or result from a specific accident), prevents the operators from being presented the information necessary for them to determine the safety status of the plant and to bring the plant to and maintain it in a safe condition following that accident.

BASES

LCO (continued)

In Table 3.3.11-1 the exception to the two channel requirement is Containment Isolation Valve Position.

Two OPERABLE channels of core exit thermocouples are required for each channel in each quadrant to provide indication of radial distribution of the coolant temperature rise across representative regions of the core. Power distribution symmetry was considered in determining the specific number and locations provided for diagnosis of local core problems. Therefore, two randomly selected thermocouples may not be sufficient to meet the two thermocouples per channel requirement in any quadrant. The two thermocouples in each channel must meet the additional requirement that one be located near the center of the core and the other near the core perimeter, such that the pair of core exit thermocouples indicate the radial temperature gradient across their core quadrant. Plant specific evaluations in response to Item II.F.2 of NUREG-0737 should have identified the thermocouple pairings that satisfy these requirements. Two sets of two thermocouples in each quadrant ensure a single failure will not disable the ability to determine the radial temperature gradient.

For loop and steam generator related variables, the required information is individual loop temperature and individual steam generator level. In these cases two channels are required to be OPERABLE for each loop of steam generator to redundantly provide the necessary information.

In the case of Containment Isolation Valve Position, the important information is the status of the containment penetrations. The LCO requires one position indicator for each active containment isolation valve. This is sufficient to redundantly verify the isolation status of each isolable penetration either via indicated status of the active valve and prior knowledge of the passive valve or via system boundary status. If a normally active containment isolation valve is known to be closed and deactivated, position indication is not needed to determine status. Therefore, the position indication for valves in this state is not required to be OPERABLE.

APPLICABILITY

The PAM instrumentation LCO is applicable in MODES 1, 2, and 3. These variables are related to the diagnosis and preplanned actions required to mitigate DBAs. The applicable DBAs are assumed to occur in MODES 1, 2, and 3. In MODES 4, 5, and 6, plant conditions are such that the likelihood of an event occurring that would require PAM instrumentation is low; therefore, PAM instrumentation is not required to be OPERABLE in these MODES.

BASES

ACTIONS

A Note has been added in the ACTIONS to clarify the application of Completion Time rules. The Conditions of this Specification may be entered independently for each Function listed in Table 3.3.11-1. The Completion Time(s) of the inoperable channel(s) of a Function will be tracked separately for each Function, starting from the time the Condition was entered for that Function.

A.1

When one or more Functions have one required channel that is inoperable, the required inoperable channel must be restored to OPERABLE status within 30 days. The 30 day Completion Time is based on operating experience and takes into account the remaining OPERABLE channel (or in the case of a Function that has only one required channel, other non-Regulatory Guide 1.97 instrument channels to monitor the Function), the passive nature of the instrument (no critical automatic action is assumed to occur from these instruments), and the low probability of an event requiring PAM instrumentation during this interval.

B.1

This Required Action specifies initiation of actions in accordance with Specification 5.6.5, which requires a written report to be submitted to the Nuclear Regulatory Commission. This report discusses the results of the root cause evaluation of the inoperability and identifies proposed restorative Required Actions. This Required Action is appropriate in lieu of a shutdown requirement, given the likelihood of plant conditions that would require information provided by this instrumentation. Also, alternative Required Actions are identified before a loss of functional capability condition occurs.

C.1

When one or more Functions have two required channels inoperable (i.e., two channels inoperable in the same Function), one channel in the Function should be restored to OPERABLE status within 7 days. The Completion Time of 7 days is based on the relatively low probability of an event requiring PAM instrumentation operation and the availability of alternate means to obtain the required information. Continuous operation with two required channels inoperable in a Function is not acceptable

BASES

ACTIONS (continued)

because the alternate indications may not fully meet all performance qualification requirements applied to the PAM instrumentation. Therefore, requiring restoration of one inoperable channel of the Function limits the risk that the PAM Function will be in a degraded condition should an accident occur.

D.1

This Required Action directs entry into the appropriate Condition referenced in Table 3.3.11-1. The applicable Condition referenced in the Table is Function dependent. Each time Required Action C.1 is not met, and the associated Completion Time has expired, Condition D is entered for that channel and provides for transfer to the appropriate subsequent Condition.

E.1 and E.2

If the Required Action and associated Completion Time of Condition D is not met, and Table 3.3.11-1 directs entry into Condition E, the plant must be brought to a MODE in which the requirements of this LCO do not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 4 within 12 hours.

The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

F.1

[At this plant, alternate means of monitoring Reactor Vessel Water Level and Containment Area Radiation have been developed and tested. These alternate means may be temporarily installed if the normal PAM channel cannot be restored to OPERABLE status within the allotted time. If these alternate means are used, the Required Action is not to shut down the plant, but rather to follow the directions of Specification 5.6.5. The report provided to the NRC should discuss the alternate means used, describe the degree to which the alternate means are equivalent to the installed PAM channels, justify the areas in which they are not equivalent, and provide a schedule for restoring the normal PAM channels.]

BASES

SURVEILLANCE REQUIREMENTS

A Note at the beginning of the Surveillance Requirementsspecifies that the following SRs apply to each PAM instrumentation Function in Table 3.3.11-1.

SR 3.3.11.1

Performance of the CHANNEL CHECK once every 31 days ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the parameter indicated on one channel to a similar parameter on other channels. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value. Significant deviations between the two instrument channels could be an indication of excessive instrument drift in one of the channels or of something even more serious. A CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

Agreement criteria are determined by the plant staff based on a combination of the channel instrument uncertainties, including indication and readability. If a channel is outside the criteria, it may be an indication that the sensor or the signal processing equipment has drifted outside its limit. If the channels are within the criteria, it is an indication that the channels are OPERABLE. If the channels are normally off scale during times when surveillance is required, the CHANNEL CHECK will only verify that they are off scale in the same direction. Off scale low current loop channels are verified to be reading at the bottom of the range and not failed downscale.

The Frequency of 31 days is based upon plant operating experience with regard to channel OPERABILITY and drift, which demonstrates that failure of more than one channel of a given Function in any 31 day interval is a rare event. The CHANNEL CHECK supplements less formal, but more frequent, checks of channel during normal operational use of the displays associated with this LCO's required channels.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.11.2

A CHANNEL CALIBRATION is performed every [18] months or approximately every refueling. CHANNEL CALIBRATION is a complete check of the instrument channel including the sensor. The Surveillance verifies the channel responds to the measured parameter within the necessary range and accuracy. A Note allows exclusion of neutron detectors from the CHANNEL CALIBRATION.

[At this unit, CHANNEL CALIBRATION shall find measurement errors are within the following acceptance criteria:]

For the Containment Area Radiation instrumentation, a CHANNEL CALIBRATION may consist of an electronic calibration of the channel, not including the detector, for range decades above 10 R/hr, and a one point calibration check of the detector below 10 R/hr with a gamma source.

Whenever a sensing element is replaced, the next required CHANNEL CALIBRATION of the resistance temperature detectors (RTD) sensors is accomplished by an inplace cross calibration that compares the other sensing elements with the recently installed sensing element.

Whenever a sensing element is replaced, the next required CHANNEL CALIBRATION of the Core Exit thermocouple sensors is accomplished by an inplace cross calibration that compares the other sensing elements with the recently installed sensing element.

The Frequency is based upon operating experience and consistency with the typical industry refueling cycle and is justified by an [18] month calibration interval for the determination of the magnitude of equipment drift.

REFERENCES

1. Plant specific document (e.g., FSAR, NRC Regulatory Guide 1.97, SER letter).

2. Regulatory Guide 1.97.

3. NUREG-0737, Supplement 1.

4. NRC Safety Evaluation Report (SER).

B 3.3 INSTRUMENTATION

B 3.3.12 Remote Shutdown System (Analog)

BASES

BACKGROUND

The Remote Shutdown System provides the control room operator with sufficient instrumentation and controls to place and maintain the unit in a safe shutdown condition from a location other than the control room. This capability is necessary to protect against the possibility that the control room becomes inaccessible. A safe shutdown condition is defined as MODE 3. With the unit in MODE 3, the [Auxiliary Feedwater (AFW) System] and the steam generator safety valves or the steam generator atmospheric dump valves can be used to remove core decay heat and meet all safety requirements. The long term supply of water for the [AFW System] and the ability to borate the Reactor Coolant System (RCS) from outside the control room allow extended operation in MODE 3.

In the event that the control room becomes inaccessible, the operators can establish control at the remote shutdown panel and place and maintain the unit in MODE 3. Not all controls and necessary transfer switches are located at the remote shutdown panel. Some controls and transfer switches will be operated locally at the switchgear, motor control panels, or other local stations. The unit automatically reaches MODE 3 following a unit shutdown and can be maintained safely in MODE 3 for an extended period of time.

The OPERABILITY of the Remote Shutdown System control and instrumentation Functions ensures that there is sufficient information available on selected plant parameters to place and maintain the plant in MODE 3, should the control room become inaccessible.

APPLICABLE SAFETY ANALYSES

The Remote Shutdown System is required to provide equipment at appropriate locations outside the control room with a capability to promptly shut down and maintain the plant in a safe condition in MODE 3.

The criteria governing the design and the specific system requirements of the Remote Shutdown System are located in 10 CFR 50, Appendix A, GDC 19, and Appendix R (Ref. 1).

The Remote Shutdown System satisfies Criterion 4 of 10 CFR 50.36(c)(2)(ii).

LCO

The Remote Shutdown System LCO provides the requirements for the OPERABILITY of the instrumentation and controls necessary to place and maintain the unit in MODE 3 from a location other than the control room. The instrumentation and controls required are listed in Table B 3.3.12-1.

BASES

LCO (continued)

The controls, instrumentation, and transfer switches are those required for:

- Core Reactivity Control (initial and long term),
- RCS Pressure Control,
- Decay Heat Removal via the [AFW System] and the safety valves or steam generator ADVs,
- RCS Inventory Control via charging flow, and
- Safety support systems for the above Functions, as well as service water, component cooling water, and onsite power including the diesel generators.

A Function of a Remote Shutdown System is OPERABLE if all instrument and control channels needed to support the remote shutdown Functions are OPERABLE. In some cases, Table B 3.3.12-1 may indicate that the required information or control capability is available from several alternate sources. In these cases, the Function is OPERABLE as long as one channel of any of the alternate information or control sources for each Function is OPERABLE.

The Remote Shutdown System instrumentation and control circuits covered by this LCO do not need to be energized to be considered OPERABLE. This LCO is intended to ensure that the instrument and control circuits will be OPERABLE if plant conditions require that the Remote Shutdown System be placed in operation.

APPLICABILITY

The Remote Shutdown System LCO is applicable in MODES 1, 2, and 3. This is required so that the unit can be placed and maintained in MODE 3 for an extended period of time from a location other than the control room.

This LCO is not applicable in MODE 4, 5, or 6. In these MODES, the unit is already subcritical and in the condition of reduced RCS energy. Under these conditions, considerable time is available to restore necessary instrument control Functions if control room instruments or control become unavailable.

BASES

ACTIONS

A Remote Shutdown System division is inoperable when each Function is not accomplished by at least one designated Remote Shutdown System channel that satisfies the OPERABILITY criteria for the channel's Function. These criteria are outlined in the LCO section of the Bases.

A Note has been added in the ACTIONS to clarify the application of Completion Time rules. The Conditions of this Specification may be entered independently for each Function. The Completion Time(s) of the inoperable channel(s)/train(s) of a Function will be tracked separately for each Function, starting from the time the Condition was entered for that Function.

<u>A.1</u>

Condition A addresses the situation where one or more channels of the Remote Shutdown System are inoperable. This includes the control and transfer switches for any required Function.

The Required Action is to restore the divisions to OPERABLE status within 30 days. The Completion Time is based on operating experience and the low probability of an event that would require evacuation of the control room.

<u>B.1 and B.2</u>

If the Required Action and associated Completion Time of Condition A are not met, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 4 within [12] hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required MODE from full power conditions in an orderly manner and without challenging plant systems.

BASES

SURVEILLANCE REQUIREMENTS

[SR 3.3.12.1

Performance of the CHANNEL CHECK once every 31 days ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the parameter indicated on one channel to a similar parameter on other channels. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value. Significant deviations between the instrument channels could be an indication of excessive instrument drift in one of the channels or of something even more serious. A CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying that the instrumentation continues to operate properly between each CHANNEL CALIBRATION. Agreement criteria are determined by the plant staff, based on a combination of the channel instrument uncertainties, including indication and readability. If a channel is outside the criteria, it may be an indication that the sensor or the signal processing equipment has drifted outside its limit. As specified in the Surveillance, a CHANNEL CHECK is only required for those channels that are normally energized. If the channels are within the criteria, it is an indication that the channels are OPERABLE. If the channels are normally off scale during times when surveillance is required, the CHANNEL CHECK will only verify that they are off scale in the same direction. Off scale low current loop channels are verified to be reading at the bottom of the range and not failed downscale.

The Frequency is based on plant operating experience that demonstrates channel failure is rare.]

SR 3.3.12.2

SR 3.3.12.2 verifies that each required Remote Shutdown System transfer switch and control circuit performs its intended function. This verification is performed from the reactor shutdown panel and locally, as appropriate. Operation of the equipment from the remote shutdown panel is not necessary. The Surveillance can be satisfied by performance of a continuity check. This will ensure that if the control room becomes inaccessible, the plant can be placed and maintained in MODE 3 from the reactor shutdown panel and the local control stations. The [18] month Frequency is based on the need to perform this Surveillance under the conditions that apply during a plant outage and the potential for an unplanned transient if the Surveillance were performed with the reactor at power. Operating experience demonstrates that Remote Shutdown System control channels seldom fail to pass the Surveillance when performed at a Frequency of once every [18] months.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.12.3

CHANNEL CALIBRATION is a complete check of the instrument channel including the sensor. The Surveillance verifies that the channel responds to the measured parameter within the necessary range and accuracy. Whenever a sensing element is replaced, the next required CHANNEL CALIBRATION of the resistance temperature detectors (RTD) sensors is accomplished by an inplace cross calibration that compares the other sensing elements with the recently installed sensing element.

The 18 month Frequency is based upon the need to perform this Surveillance under the conditions that apply during a plant outage and the potential for an unplanned transient if the Surveillance were performed with the reactor at power.

The SR is modified by a Note, which excludes neutron detectors from the CHANNEL CALIBRATION.

[SR 3.3.12.4

SR 3.3.12.4 is the performance of a CHANNEL FUNCTIONAL TEST every 18 months. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions. This Surveillance should verify the OPERABILITY of the reactor trip circuit breaker (RTCB) open/closed indication on the remote shutdown panels by actuating the RTCBs. The Frequency of 18 months was chosen because the RTCBs cannot be exercised while the unit is at power. Operating experience has shown that these components usually pass the Surveillance when performed at a Frequency of once every 18 months. Therefore, the Frequency was concluded to be acceptable from a reliability standpoint.]

REFERENCES

1. 10 CFR 50, Appendix A, GDC 19, and Appendix R.
2. NRC Safety Evaluation Report (SER).

Table B 3.3.12-1 (page 1 of 1)
Remote Shutdown System Instrumentation and Controls

---NOTE---
This Table is for illustration purposes only. It does not attempt to encompass every Function used at every unit, but does contain the types of Functions commonly found.

		FUNCTION/INSTRUMENT OR CONTROL PARAMETER	REQUIRED NUMBER OF DIVISIONS
1.	Reactivity Control		
	a.	Log Power Neutron Flux	[1]
	b.	Source Range Neutron Flux	[1]
	c.	Reactor Trip Circuit Breaker Position	[1 per trip breaker]
	d.	Manual Reactor Trip	[2]
2.	Reactor Coolant System Pressure Control		
	a.	Pressurizer Pressure or RCS Wide Range Pressure	[1]
	b.	Pressurizer Power Operated Relief Valve Control and Block Valve Control	[1, controls must be for power operated relief valve and block valves on same line]
3.	Decay Heat Removal via Steam Generators		
	a.	Reactor Coolant\ Hot Leg Temperature	[1 per loop]
	b.	Reactor Coolant Cold Leg Temperature	[1 per loop]
	c.	Auxiliary Feedwater Controls	[1]
	d.	Steam Generator Pressure	[1 per steam generator]
	e.	Steam Generator Level or Auxiliary Feedwater Flow	[1 per steam generator]
	f.	Condensate Storage Tank Level	[1]
4.	Reactor Coolant System Inventory Control		
	a.	Pressurizer Level	[1]
	b.	Reactor Coolant Charging Pump Controls	[1]

---REVIEWER'S NOTE---
The number of channels that fulfill GDC 19 requirements for the number of OPERABLE channels required depends upon the plant's licensing basis as described in the NRC plant specific Safety Evaluation Report (SER) (Ref. 2). Generally, two divisions are required to be OPERABLE. However, only one channel is required if the plant has justified such a design and the NRC's SER accepted the justification.

B 3.3 INSTRUMENTATION

B 3.3.13 [Logarithmic] Power Monitoring Channels (Analog)

BASES

BACKGROUND

The [logarithmic] power monitoring channels provide neutron flux power indication from < 1E-7% RTP to > 100% RTP. They also provide reactor protection when the reactor trip circuit breakers (RTCBs) are shut, in the form of a Power Rate of Change - High trip (analog plants) or a [Logarithmic] Power Level - High trip (digital plants).

This LCO addresses MODES 3, 4, and 5 with the RTCBs open. When the RTCBs are shut, the [logarithmic] power monitoring channels are addressed by LCO 3.3.2, "Reactor Protective System (RPS) Instrumentation - Shutdown."

When the RTCBs are open, two of the four wide range power channels must be available to monitor neutron flux power. In this application, the RPS channels need not be OPERABLE since the reactor trip Function is not required. By monitoring neutron flux power when the RTCBs are open, loss of SDM caused by boron dilution can be detected as an increase in flux. Alarms are also provided when power increases above the fixed bistable setpoints. For plants employing separate post accident, [logarithmic] nuclear instrumentation channels with adequate range, these can be substituted for the [logarithmic] power range channels. Two channels must be OPERABLE to provide single failure protection and to facilitate detection of channel failure by providing CHANNEL CHECK capability.

APPLICABLE SAFETY ANALYSES

The [logarithmic] power monitoring channels are necessary to monitor core reactivity changes. They are the primary means for detecting and triggering operator actions to respond to reactivity transients initiated from conditions in which the RPS is not required to be OPERABLE. They also trigger operator actions to anticipate RPS actuation in the event of reactivity transients starting from shutdown or low power conditions. The [logarithmic] power monitoring channel's LCO requirements support compliance with 10 CFR 50, Appendix A, GDC 13 (Ref. 1). The FSAR, Chapters [7] and [15] (Refs. 2 and 3, respectively), describes the specific [logarithmic] power monitoring channel features that are critical to comply with the GDC.

The OPERABILITY of [logarithmic] power monitoring channels is necessary to meet the assumptions of the safety analyses and provide for the mitigation of accident and transient conditions.

The [logarithmic] power monitoring channels satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO	The LCO on the [logarithmic] power monitoring channels ensures that adequate information is available to verify core reactivity conditions while shut down. A minimum of two [logarithmic] power monitoring channels are required to be OPERABLE. Some plants may have either four or six channels capable of performing this function. In these cases, multiple failures may be tolerated while the plants are still complying with LCO requirements.
APPLICABILITY	In MODES 3, 4, and 5, with RTCBs open or the Control Element Assembly (CEA) Drive System not capable of CEA withdrawal, [logarithmic] power monitoring channels must be OPERABLE to monitor core power for reactivity changes. In MODES 1 and 2, and in MODES 3, 4, and 5 with the RTCBs shut and the CEAs capable of withdrawal, the [logarithmic] power monitoring channels are addressed as part of the RPS in LCO 3.3.1, "Reactor Protective System (RPS) Instrumentation - Operating." The requirements for source range neutron flux monitoring in MODE 6 are addressed in LCO 3.9.2, "Nuclear Instrumentation." The source range nuclear instrumentation channels provide neutron flux coverage extending an additional one to two decades below the [logarithmic] channels for use during refueling, when neutron flux may be extremely low. They are built into the [logarithmic] neutron flux channels in the analog plants and in many of the post accident channels used in both the digital and analog plants.
ACTIONS	<u>A.1 and A.2</u> With one required channel inoperable, it may not be possible to perform a CHANNEL CHECK to verify that the other required channel is OPERABLE. Therefore, with one or more required channels inoperable, the [logarithmic] power monitoring Function cannot be reliably performed. Consequently, the Required Actions are the same for one required channel inoperable or more than one required channel inoperable. The absence of reliable neutron flux indication makes it difficult to ensure SDM is maintained. Required Action [A.1] is modified by a Note to indicate that normal plant control operations that individually add limited positive reactivity (e.g., temperature or boron fluctuations associated with RCS inventory management or temperature control) are not precluded by this Action, provided they are accounted for in the calculated SDM.

BASES

ACTIONS (continued)

SDM must be verified periodically to ensure that it is being maintained. Both required channels must be restored as soon as possible. The initial Completion Time of 4 hours and once every 12 hours thereafter to perform SDM verification takes into consideration that Required Action A.1 eliminates many of the means by which SDM can be reduced. These Completion Times are also based on operating experience in performing the Required Actions and the fact that plant conditions will change slowly.

SURVEILLANCE REQUIREMENTS

SR 3.3.13.1

SR 3.3.13.1 is the performance of a CHANNEL CHECK on each required channel every 12 hours. A CHANNEL CHECK is normally a comparison of the parameter indicated on one channel to a similar parameter on other channels. It is based upon the assumption that instrument channels monitoring the same parameter should read approximately the same value. Significant deviations between instrument channels could be an indication of excessive instrument drift in one of the channels or of something even more serious. CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying that the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

Agreement criteria are determined by the plant staff and should be based on a combination of the channel instrument uncertainties including control isolation, indication, and readability. If a channel is outside the criteria, it may be an indication that the transmitter or the signal processing equipment has drifted outside its limits. If the channels are within the criteria, it is an indication that the channels are OPERABLE.

The Frequency, about once every shift, is based on operating experience that demonstrates the rarity of channel failure. Since the probability of two random failures in redundant channels in any 12 hour period is extremely low, CHANNEL CHECK minimizes the chance of loss of protective function due to failure of redundant channels. CHANNEL CHECK supplements less formal, but more frequent, checks of channel OPERABILITY during normal operational use of displays associated with the LCO required channels.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.13.2

A CHANNEL FUNCTIONAL TEST is performed every [92] days to ensure that the entire channel is capable of properly indicating neutron flux. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions. Internal test circuitry is used to feed preadjusted test signals into the preamplifier to verify channel alignment. It is not necessary to test the detector, because generating a meaningful test signal is difficult; the detectors are of simple construction, and any failures in the detectors will be apparent as change in channel output. This Frequency is the same as that employed for the same channels in the other applicable MODES. [At this unit, the channel trip Functions tested by the CHANNEL FUNCTIONAL TEST are as follows:]

SR 3.3.13.3

SR 3.3.13.3 is the performance of a CHANNEL CALIBRATION. A CHANNEL CALIBRATION is performed every [18] months. The Surveillance is a complete check and readjustment of the [logarithmic] power channel from the preamplifier input through to the remote indicators. The Surveillance verifies that the channel responds to a measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drift between successive calibrations to ensure that the channel remains operational between successive surveillances. CHANNEL CALIBRATIONS must be performed consistent with the plant specific setpoint analysis.

This SR is modified by a Note to indicate that it is not necessary to test the detector because generating a meaningful test signal is difficult; the detectors are of simple construction, and any failures in the detectors will be apparent as change in channel output. This Frequency is the same as that employed for the same channels in the other applicable MODES.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 13.
2. FSAR, Chapter [7].
3. FSAR, Chapter [15].

B 3.3 INSTRUMENTATION

B 3.3.1 Reactor Protective System (RPS) Instrumentation - Operating (Digital)

BASES

BACKGROUND

The RPS initiates a reactor trip to protect against violating the core specified acceptable fuel design limits and breaching the reactor coolant pressure boundary (RCPB) during anticipated operational occurrences (AOOs). By tripping the reactor, the RPS also assists the Engineered Safety Features (ESF) systems in mitigating accidents.

The protection and monitoring systems have been designed to ensure safe operation of the reactor. This is achieved by specifying limiting safety system settings (LSSS) in terms of parameters directly monitored by the RPS, as well as LCOs on other reactor system parameters and equipment performance.

Technical Specifications are required by 10 CFR 50.36 to contain LSSS defined by the regulation as "...settings for automatic protective devices...so chosen that automatic protective actions will correct the abnormal situation before a Safety Limit (SL) is exceeded." The Analytic Limit is the limit of the process variable at which a safety action is initiated, as established by the safety analysis, to ensure that a SL is not exceeded. Any automatic protection action that occurs on reaching the Analytic Limit therefore ensures that the SL is not exceeded. However, in practice, the actual settings for automatic protective devices must be chosen to be more conservative than the Analytic Limit to account for instrument loop uncertainties related to the setting at which the automatic protective action would actually occur.

The trip setpoint is a predetermined setting for a protective device chosen to ensure automatic actuation prior to the process variable reaching the Analytic Limit and thus ensuring that the SL would not be exceeded. As such, the trip setpoint accounts for uncertainties in setting the device (e.g., calibration), uncertainties in how the device might actually perform (e.g., repeatability), changes in the point of action of the device over time (e.g., drift during surveillance intervals), and any other factors which may influence its actual performance (e.g., harsh accident environments). In this manner, the trip setpoint plays an important role in ensuring that SLs are not exceeded. As such, the trip setpoint meets the definition of an LSSS (Ref. 1) and could be used to meet the requirement that they be contained in the Technical Specifications.

BASES

BACKGROUND (continued)

Technical Specifications contain values related to the OPERABILITY of equipment required for safe operation of the facility. OPERABLE is defined in Technical Specifications as "...being capable of performing its safety function(s)." For automatic protective devices, the required safety function is to ensure that a SL is not exceeded and therefore the LSSS as defined by 10 CFR 50.36 is the same as the OPERABILITY limit for these devices. However, use of the trip setpoint to define OPERABILITY in Technical Specifications and its corresponding designation as the LSSS required by 10 CFR 50.36 would be an overly restrictive requirement if it were applied as an OPERABILITY limit for the "as found" value of a protective device setting during a Surveillance. This would result in Technical Specification compliance problems, as well as reports and corrective actions required by the rule which are not necessary to ensure safety. For example, an automatic protective device with a setting that has been found to be different from the trip setpoint due to some drift of the setting may still be OPERABLE since drift is to be expected. This expected drift would have been specifically accounted for in the setpoint methodology for calculating the trip setpoint and thus the automatic protective action would still have ensured that the SL would not be exceeded with the "as found" setting of the protective device. Therefore, the device would still be OPERABLE since it would have performed its safety function and the only corrective action required would be to reset the device to the trip setpoint to account for further drift during the next surveillance interval.

Use of the trip setpoint to define "as found" OPERABILITY and its designation as the LSSS under the expected circumstances described above would result in actions required by both the rule and Technical Specifications that are clearly not warranted. However, there is also some point beyond which the device would have not been able to perform its function due, for example, to greater than expected drift. This value needs to be specified in the Technical Specifications in order to define OPERABILITY of the devices and is designated as the Allowable Value which, as stated above, is the same as the LSSS.

The Allowable Valuable specified in Table 3.3.1-1 serves as the LSSS such that a channel is OPERABLE if the trip setpoint is found not to exceed the Allowable Value. As such, the Allowable Value differs from the trip setpoint by an amount primarily equal to the expected instrument loop uncertainties, such as drift, during the surveillance interval. In this manner, the actual setting of the device will still meet the LSSS definition and ensure that a SL is not exceeded at any given point of time as long as the device has not drifted beyond that expected during the

BASES

BACKGROUND (continued)

surveillance interval. If the actual setting of the device is found to have exceeded the Allowable Value the device would be considered inoperable from a Technical Specification perspective. This requires corrective action including those actions required by 10 CFR 50.36 when automatic protective devices do not function as required. Note that, although the channel is "OPERABLE" under these circumstances, the trip setpoint should be left adjusted to a value within the established trip setpoint calibration tolerance band, in accordance with uncertainty assumptions stated in the referenced setpoint methodology (as-left criteria), and confirmed to be operating within the statistical allowances of the uncertainty terms assigned.

During AOOs, which are those events expected to occur one or more times during the plant life, the acceptable limits are:

- The departure from nucleate boiling ratio (DNBR) shall be maintained above the Safety Limit (SL) value to prevent departure from nucleate boiling (DNB),
- Fuel centerline melting shall not occur, and
- The Reactor Coolant System (RCS) pressure SL of 2750 psia shall not be exceeded.

Maintaining the parameters within the above values ensures that the offsite dose will be within the 10 CFR 50 (Ref. 2) and 10 CFR 100 (Ref. 3) criteria during AOOs.

Accidents are events that are analyzed even though they are not expected to occur during the plant life. The acceptable limit during accidents is that the offsite dose shall be maintained within an acceptable fraction of 10 CFR 100 (Ref. 3) limits. Different accident categories allow a different fraction of these limits based on probability of occurrence. Meeting the acceptable dose limit for an accident category is considered having acceptable consequences for that event.

The RPS is segmented into four interconnected modules. These modules are:

- Measurement channels,

BASES

BACKGROUND (continued)

- Bistable trip units,
- RPS Logic, and
- Reactor trip circuit breakers (RTCBs).

This LCO addresses measurement channels and bistable trip units. It also addresses the automatic bypass removal feature for those trips with operating bypasses. The RPS Logic and RTCBs are addressed in LCO 3.3.4, "Reactor Protective System (RPS) Logic and Trip Initiation." The CEACs are addressed in LCO 3.3.3, "Control Element Assembly Calculators (CEACs)."

Measurement Channels

Measurement channels, consisting of field transmitters or process sensors and associated instrumentation, provide a measurable electronic signal based upon the physical characteristics of the parameter being measured.

The excore nuclear instrumentation, the core protection calculators (CPCs), and the CEACs, though complex, are considered components in the measurement channels of the Linear Power Level - High, Logarithmic Power Level - High, DNBR - Low, and Local Power Density (LPD) - High trips.

Four identical measurement channels, designated channels A through D, with electrical and physical separation, are provided for each parameter used in the generation of trip signals, with the exception of the control element assembly (CEA) position indication used in the CPCs. Each measurement channel provides input to one or more RPS bistables within the same RPS channel. In addition, some measurement channels may also be used as inputs to Engineered Safety Features Actuation System (ESFAS) bistables, and most provide indication in the control room. Measurement channels used as an input to the RPS are not used for control functions.

When a channel monitoring a parameter exceeds a predetermined setpoint, indicating an unsafe condition, the bistable monitoring the parameter in that channel will trip. Tripping bistables monitoring the same parameter in two or more channels will de-energize Matrix Logic, which in turn de-energizes the Initiation Logic. This causes all eight RTCBs to open, interrupting power to the CEAs, allowing them to fall into the core.

BASES

BACKGROUND (continued)

Three of the four measurement and bistable channels are necessary to meet the redundancy and testability of 10 CFR 50, Appendix A, GDC 21 (Ref. 2). The fourth channel provides additional flexibility by allowing one channel to be removed from service (trip channel bypass) for maintenance or testing while still maintaining a minimum two-out-of-three logic. Thus, even with a channel inoperable, no single additional failure in the RPS can either cause an inadvertent trip or prevent a required trip from occurring.

----------------------------------REVIEWER'S NOTE-----------------------------------
In order to take full advantage of the four channel design, adequate channel to channel independence must be demonstrated and approved by the NRC staff. Plants not currently licensed so as to credit four channel independence and that desire this capability must have approval of the NRC staff documented by an NRC Safety Evaluation Report (SER) (Ref. 4).

Adequate channel to channel independence includes physical and electrical independence of each channel from the others. This allows operation in two-out-of-three logic with one channel removed from service until following the next MODE 5 entry. Since no single failure will either cause or prevent a protective system actuation, and no protective channel feeds a control, this arrangement meets the requirements of IEEE Standard 279-1971 (Ref. 5).

The CPCs perform the calculations required to derive the DNBR and LPD parameters and their associated RPS trips. Four separate CPCs perform the calculations independently, one for each of the four RPS channels. The CPCs provide outputs to drive display indications (DNBR margin, LPD margin, and calibrated neutron flux power levels) and provide DNBR - Low and LPD - High pretrip and trip signals. The CPC channel outputs for the DNBR - Low and LPD - High trips operate contacts in the Matrix Logic in a manner identical to the other RPS trips.

Each CPC receives the following inputs:

- Hot leg and cold leg temperatures,
- Pressurizer pressure,
- Reactor coolant pump speed,

BASES

BACKGROUND (continued)

- Excore neutron flux levels,
- Target CEA positions, and
- CEAC penalty factors.

Each CPC is programmed with "addressable constants." These are various alignment values, correction factors, etc., that are required for the CPC computations. They can be accessed for display or for the purpose of changing them as necessary.

The CPCs use this constant and variable information to perform a number of calculations. These include the calculation of CEA group and subgroup deviations (and the assignment of conservative penalty factors), correction and calculation of average axial power distribution (APD) (based on excore flux levels and CEA positions), calculation of coolant flow (based on pump speed), and calculation of calibrated average power level (based on excore flux levels and ΔT power).

The DNBR calculation considers primary pressure, inlet temperature, coolant flow, average power, APD, radial peaking factors, and CEA deviation penalty factors from the CEACs to calculate the state of the limiting (hot) coolant channel in the core. A DNBR - Low trip occurs when the calculated value reaches the minimum DNBR trip setpoint.

The LPD calculation considers APD, average power, radial peaking factors (based upon target CEA position), and CEAC penalty factors to calculate the current value of compensated peak power density. An LPD - High trip occurs when the calculated value reaches the trip setpoint. The four CPC channels provide input to the four DNBR - Low and four LPD - High RPS trip channels. They effectively act as the sensor (using many inputs) for these trips.

The CEACs perform the calculations required to determine the position of CEAs within their subgroups for the CPCs. Two independent CEACs compare the position of each CEA to its subgroup position. If a deviation is detected by either CEAC, an annunciator sounds and appropriate "penalty factors" are transmitted to all CPCs. These penalty factors conservatively adjust the effective operating margins to the DNBR - Low and LPD - High trips. Each CEAC also drives a single cathode ray tube (CRT), which is switchable between CEACs. The CRT displays individual CEA positions and current values of the penalty factors from the selected CEAC.

BASES

BACKGROUND (continued)

Each CEA has two separate reed switch assemblies mounted outside the RCPB. Each of the two CEACs receives CEA position input from one of the two reed switch position transmitters on each CEA, so that the position of all CEAs is independently monitored by both CEACs.

CEACs are addressed in LCO 3.3.3.

Bistable Trip Units

Bistable trip units, mounted in the Plant Protection System (PPS) cabinet, receive an analog input from the measurement channels. They compare the analog input to trip setpoints and provide contact output to the Matrix Logic. They also provide local trip indication and remote annunciation.

There are four channels of bistables, designated A, B, C, and D, for each RPS parameter, one for each measurement channel. Bistables de-energize when a trip occurs, in turn de-energizing bistable relays mounted in the PPS relay card racks.

The contacts from these bistable relays are arranged into six coincidence matrices, comprising the Matrix Logic. If bistables monitoring the same parameter in at least two channels trip, the Matrix Logic will generate a reactor trip (two-out-of-four logic).

Some measurement channels provide contact outputs to the PPS. In these cases, there is no bistable card, and opening the contact input directly de-energizes the associated bistable relays. These include the Loss of Load trip and the CPC generated DNBR - Low and LPD - High trips.

The trip setpoints used in the bistables are based on the analytical limits derived from the accident analysis (Ref. 6). The selection of these trip setpoints is such that adequate protection is provided when all sensor and processing time delays are taken into account. To allow for calibration tolerances, instrumentation uncertainties, instrument drift, and severe environment errors for those RPS channels that must function in harsh environments as defined by 10 CFR 50.49 (Ref. 7), Allowable Values specified in Table 3.3.1-1, in the accompanying LCO, are

BASES

BACKGROUND (continued)

conservatively adjusted with respect to the analytical limits. A detailed description of the methodology used to calculate the trip setpoints, including their explicit uncertainties, is provided in "Plant Protection System Selection of Trip Setpoint Values" (Ref. 8). The nominal trip setpoint entered into the bistable is normally still more conservative than that specified by the Allowable Value to account for changes in random measurement errors detectable by a CHANNEL FUNCTIONAL TEST. One example of such a change in measurement error is drift during the interval between surveillances. A channel is inoperable if its actual setpoint is not within its Allowable Value.

Setpoints in accordance with the Allowable Value will ensure that SLs of Chapter 2.0, "SAFETY LIMITS (SLs)," are not violated during AOOs, and the consequences of DBAs will be acceptable, providing the plant is operated from within the LCOs at the onset of the AOO or DBA and the equipment functions as designed.

Note that in LCO 3.3.1, the Allowable Values of Table 3.3.1-1 are the LSSS.

Functional testing of the entire RPS, from bistable input through the opening of individual sets of RTCBs, can be performed either at power or shutdown and is normally performed on a quarterly basis. Nuclear instrumentation, the CPCs, and the CEACs can be similarly tested. FSAR, Section [7.2] (Ref. 9), provides more detail on RPS testing. Processing transmitter calibration is normally performed on a refueling basis.

<u>RPS Logic</u>

The RPS Logic, addressed in LCO 3.3.4, consists of both Matrix and Initiation Logic and employs a scheme that provides a reactor trip when bistables in any two of the four channels sense the same input parameter trip. This is called a two-out-of-four trip logic.

Bistable relay contact outputs from the four channels are configured into six logic matrices. Each logic matrix checks for a coincident trip in the same parameter in two bistable channels. The matrices are designated the AB, AC, AD, BC, BD, and CD matrices to reflect the bistable channels being monitored. Each logic matrix contains four normally energized matrix relays. When a coincidence is detected, consisting of a trip in the same Function in the two channels being monitored by the logic matrix, all four matrix relays de-energize.

BASES

BACKGROUND (continued)

The matrix relay contacts are arranged into trip paths, with one of the four matrix relays in each matrix opening contacts in one of the four trip paths. Each trip path provides power to one of the four normally energized RTCB control relays (K1, K2, K3, and K4). The trip paths thus each have six contacts in series, one from each matrix, and perform a logical OR function, opening the RTCBs if any one or more of the six logic matrices indicate a coincidence condition.

Each trip path is responsible for opening one set of two of the eight RTCBs. The RTCB control relays (K-relays), when de-energized, interrupt power to the breaker undervoltage trip attachments and simultaneously apply power to the shunt trip attachments on each of the two breakers. Actuation of either the undervoltage or shunt trip attachment is sufficient to open the RTCB and interrupt power from the motor generator (MG) sets to the control element drive mechanisms (CEDMs).

When a coincidence occurs in two RPS channels, all four matrix relays in the affected matrix de-energize. This in turn de-energizes all four breaker control relays, which simultaneously de-energize the undervoltage and energize the shunt trip attachments in all eight RTCBs, tripping them open.

Matrix Logic refers to the matrix power supplies, trip channel bypass contacts, and interconnecting matrix wiring between bistable relay cards, up to but not including the matrix relays. Matrix contacts on the bistable relay cards are excluded from the Matrix Logic definition, since they are addressed as part of the measurement channel.

The Initiation Logic consists of the trip path power source, matrix relays and their associated contacts, all interconnecting wiring, and solid state (auxiliary) relays through the K-relay contacts in the RTCB control circuitry.

It is possible to change the two-out-of-four RPS Logic to a two-out-of-three logic for a given input parameter in one channel at a time by trip channel bypassing select portions of the Matrix Logic. Trip channel bypassing a bistable effectively shorts the bistable relay contacts in the three matrices associated with that channel. Thus, the bistables will

BASES

BACKGROUND (continued)

function normally, producing normal trip indication and annunciation, but a reactor trip will not occur unless two additional channels indicate a trip condition. Trip channel bypassing can be simultaneously performed on any number of parameters in any number of channels, providing each parameter is bypassed in only one channel at a time. An interlock prevents simultaneous trip channel bypassing of the same parameter in more than one channel. Trip channel bypassing is normally employed during maintenance or testing.

Two-out-of-three logic also prevents inadvertent trips caused by any single channel failure in a trip condition.

In addition to the trip channel bypasses, there are also operating bypasses on select RPS trips. These bypasses are enabled manually in all four RPS channels when plant conditions do not warrant the specific trip protection. All operating bypasses are automatically removed when enabling bypass conditions are no longer satisfied. Operating bypasses are normally implemented in the bistable, so that normal trip indication is also disabled. Trips with operating bypasses include Pressurizer Pressure - Low, Logarithmic Power Level - High, Reactor Coolant Flow - Low, and CPC (DNBR - Low and LPD - High).

The Loss of Load trip bypass is automatically enabled and disabled.

Reactor Trip Circuit Breakers (RTCBs)

The reactor trip switchgear, addressed in LCO 3.3.4, consists of eight RTCBs, which are operated in four sets of two breakers (four channels). Power input to the reactor trip switchgear comes from two full capacity MG sets operated in parallel, such that the loss of either MG set does not de-energize the CEDMs. There are two separate CEDM power supply buses, each bus powering half of the CEDMs. Power is supplied from the MG sets to each bus via two redundant paths (trip legs). Trip legs 1A and 1B supply power to CEDM bus 1. Trip legs 2A and 2B supply power to CEDM bus 2. This ensures that a fault or the opening of a breaker in one trip leg (i.e., for testing purposes) will not interrupt power to the CEDM buses.

Each of the four trip legs consists of two RTCBs in series. The two RTCBs within a trip leg are actuated by separate initiation circuits.

BASES

BACKGROUND (continued)

The eight RTCBs are operated as four sets of two breakers (four channels). For example, if a breaker receives an open signal in trip leg A (for CEDM bus 1), an identical breaker in trip leg B (for CEDM bus 2) will also receive an open signal. This arrangement ensures that power is interrupted to both CEDM buses, thus preventing trip of only half of the CEAs (a half trip). Any one inoperable breaker in a channel will make the entire channel inoperable.

Each set of RTCBs is operated by either a manual reactor trip push button or an RPS actuated K-relay. There are four Manual Trip push buttons, arranged in two sets of two. Depressing both push buttons in either set will result in a reactor trip.

When a Manual Trip is initiated using the control room push buttons, the RPS trip paths and K-relays are bypassed, and the RTCB undervoltage and shunt trip attachments are actuated independent of the RPS.

Manual Trip circuitry includes the push button and interconnecting wiring to both RTCBs necessary to actuate both the undervoltage and shunt trip attachments but excludes the K-relay contacts and their interconnecting wiring to the RTCBs, which are considered part of the Initiation Logic.

Functional testing of the entire RPS, from bistable input through the opening of individual sets of RTCBs, can be performed either at power or shutdown and is normally performed on a quarterly basis. FSAR, Section [7.2] (Ref. 9), explains RPS testing in more detail.

APPLICABLE SAFETY ANALYSES

Design Basis Definition

The RPS is designed to ensure that the following operational criteria are met:

- The associated actuation will occur when the parameter monitored by each channel reaches its setpoint and the specific coincidence logic is satisfied,

- Separation and redundancy are maintained to permit a channel to be out of service for testing or maintenance while still maintaining redundancy within the RPS instrumentation network.

Each of the analyzed accidents and transients can be detected by one or more RPS Functions. The accident analysis takes credit for most of the RPS trip Functions. Those functions for which no credit is taken, termed equipment protective functions, are not needed from a safety perspective.

BASES

APPLICABLE SAFETY ANALYSES (continued)

Each RPS setpoint is chosen to be consistent with the function of the respective trip. The basis for each trip setpoint falls into one of three general categories:

Category 1: To ensure that the SLs are not exceeded during AOOs,

Category 2: To assist the ESFAS during accidents, and

Category 3: To prevent material damage to major plant components (equipment protective).

The RPS maintains the SLs during AOOs and mitigates the consequences of DBAs in all MODES in which the RTCBs are closed.

Each of the analyzed transients and accidents can be detected by one or more RPS Functions. Functions not specifically credited in the accident analysis are part of the NRC staff approved licensing basis for the plant. Noncredited Functions include the Loss of Load. This trip is purely equipment protective, and its use minimizes the potential for equipment damage.

The specific safety analysis applicable to each protective function are identified below:

1. <u>Linear Power Level - High</u>

   The Linear Power Level - High trip provides protection against core damage during the following events:

   - Uncontrolled CEA Withdrawal From Low Power (AOO),
   - Uncontrolled CEA Withdrawal at Power (AOO), and
   - CEA Ejection (Accident).

2. <u>Logarithmic Power Level - High</u>

   The Logarithmic Power Level - High trip protects the integrity of the fuel cladding and helps protect the RCPB in the event of an unplanned criticality from a shutdown condition.

BASES

APPLICABLE SAFETY ANALYSES (continued)

In MODES 2, 3, 4, and 5, with the RTCBs closed and the CEA Drive System capable of CEA withdrawal, protection is required for CEA withdrawal events originating when logarithmic power is < 1E-4%. For events originating above this power level, other trips provide adequate protection.

MODES 3, 4, and 5, with the RTCBs closed, are addressed in LCO 3.3.2, "Reactor Protective System (RPS) Instrumentation - Shutdown."

In MODES 3, 4, or 5, with the RTCBs open or the CEAs not capable of withdrawal, the Logarithmic Power Level - High trip does not have to be OPERABLE. However, the indication and alarm portion of two logarithmic channels must be OPERABLE to ensure proper indication of neutron population and to indicate a boron dilution event. The indication and alarm functions are addressed in LCO 3.3.13, "[Logarithmic] Power Monitoring Channels."

3. Pressurizer Pressure - High

The Pressurizer Pressure - High trip provides protection for the high RCS pressure SL. In conjunction with the pressurizer safety valves and the main steam safety valves (MSSVs), it provides protection against overpressurization of the RCPB during the following events:

- Loss of Electrical Load Without a Reactor Trip Being Generated by the Turbine Trip (AOO),
- Loss of Condenser Vacuum (AOO),
- CEA Withdrawal From Low Power Conditions (AOO),
- Chemical and Volume Control System Malfunction (AOO), and
- Main Feedwater System Pipe Break (Accident).

4. Pressurizer Pressure - Low

The Pressurizer Pressure - Low trip is provided to trip the reactor to assist the ESF System in the event of loss of coolant accidents (LOCAs). During a LOCA, the SLs may be exceeded; however, the consequences of the accident will be acceptable. A Safety Injection Actuation Signal (SIAS) and a Containment Isolation Actuation Signal (CIAS) are initiated simultaneously.

BASES

APPLICABLE SAFETY ANALYSES (continued)

5. Containment Pressure - High

The Containment Pressure - High trip prevents exceeding the containment design pressure psig during a design basis LOCA or main steam line break (MSLB) accident. During a LOCA or MSLB the SLs may be exceeded; however, the consequences of the accident will be acceptable. An SIAS and CIAS are initiated simultaneously.

6, 7. Steam Generator Pressure - Low

The Steam Generator #1 Pressure - Low and Steam Generator #2 Pressure - Low trips provide protection against an excessive rate of heat extraction from the steam generators and resulting rapid, uncontrolled cooldown of the RCS. This trip is needed to shut down the reactor and assist the ESF System in the event of an MSLB or main feedwater line break accident. A main steam isolation signal (MSIS) is initiated simultaneously.

8, 9. Steam Generator Level – Low

The Steam Generator #1 Level - Low and Steam Generator #2 Level - Low trips ensure that a reactor trip signal is generated for the following events to help prevent exceeding the design pressure of the RCS due to the loss of the heat sink:

- Inadvertent Opening of a Steam Generator Atmospheric Dump Valve (AOO),
- Loss of Normal Feedwater Event (AOO), and
- Feedwater System Pipe Break (Accident).

10, 11. Reactor Coolant Flow – Low

The Reactor Coolant Flow, Steam Generator #1 - Low and Reactor Coolant Flow, Steam Generator #2 - Low trips provides protection against an RCP Sheared Shaft Event. The DNBR limit may be exceeded during this event; however, the trip ensures the consequences are acceptable.

BASES

APPLICABLE SAFETY ANALYSES (continued)

12. Loss of Load

The Loss of Load (turbine stop valve control oil pressure) is anticipatory for the loss of heat removal capabilities for the secondary system following a turbine trip. The Loss of Load trip prevents lifting the pressurizer safety valves and the main steam line safety valves in the event of a turbine generator trip. Thus, the trip minimizes the pressure or temperature transient on the reactor by initiating a trip well before the Pressurizer Pressure - High and safety valve setpoints are reached.

The RPS Loss of Load reactor trip channels receive their input from sensors mounted on high pressure turbine stop valve (TSV) actuators. Since there are four TSVs, one actuator per TSV and one sensor per actuator, each sensor sends its signal to a different RPS channel. When the control oil pressure drops to the appropriate setpoint, a reactor trip signal is generated.

13. Local Power Density – High

The CPCs perform the calculations required to derive the DNBR and LPD parameters and their associated RPS trips. The DNBR - Low and LPD - High trips provide plant protection during the following AOOs and assist the ESF systems in the mitigation of the following accidents.

The LPD - High trip provides protection against fuel centerline melting due to the occurrence of excessive local power density peaks during the following AOOs:

- Decrease in Feedwater Temperature,
- Increase in Feedwater Flow,
- Increased Main Steam Flow (not due to the steam line rupture) Without Turbine Trip,
- Uncontrolled CEA Withdrawal From Low Power,
- Uncontrolled CEA Withdrawal at Power, and
- CEA Misoperation; Single Part Length CEA Drop.

BASES

APPLICABLE SAFETY ANALYSES (continued)

For the events listed above (except CEA Misoperation; Single Part Length CEA Drop), DNBR - Low will trip the reactor first, since DNB would occur before fuel centerline melting would occur.

14. Departure from Nucleate Boiling Ratio (DNBR) - Low

The CPCs perform the calculations required to derive the DNBR and LPD parameters and their associated RPS trips. The DNBR - Low and LPD - High trips provide plant protection during the following AOOs and assist the ESF systems in the mitigation of the following accidents.

The DNBR - Low trip provides protection against core damage due to the occurrence of locally saturated conditions in the limiting (hot) channel during the following events and is the primary reactor trip (trips the reactor first) for these events:

- Decrease in Feedwater Temperature,
- Increase in Feedwater Flow,
- Increased Main Steam Flow (not due to steam line rupture) Without Turbine Trip,
- Increased Main Steam Flow (not due to steam line rupture) With a Concurrent Single Failure of an Active Component,
- Steam Line Break With Concurrent Loss of Offsite AC Power,
- Loss of Normal AC Power,
- Partial Loss of Forced Reactor Coolant Flow,
- Total Loss of Forced Reactor Coolant Flow,
- Single Reactor Coolant Pump (RCP) Shaft Seizure,
- Uncontrolled CEA Withdrawal From Low Power,
- Uncontrolled CEA Withdrawal at Power,
- CEA Misoperation; Full Length CEA Drop,

BASES

APPLICABLE SAFETY ANALYSES (continued)

- CEA Misoperation; Part Length CEA Subgroup Drop,
- Primary Sample or Instrument Line Break, and
- Steam Generator Tube Rupture.

In the above list, only the steam generator tube rupture, the RCP shaft seizure, and the sample or instrument line break are accidents. The rest are AOOs.

Interlocks/Bypasses

The bypasses and their Allowable Values are addressed in footnotes to Table 3.3.1-1. They are not otherwise addressed as specific Table entries.

The automatic bypass removal features must function as a backup to manual actions for all safety related trips to ensure the trip Functions are not operationally bypassed when the safety analysis assumes the Functions are not bypassed. The basis for each of the operating bypasses is discussed under individual trips in the LCO section:

a. Loss of Load,

b. Logarithmic Power Level - High,

c. Reactor Coolant Flow - Low,

d. DNBR - Low and LPD - High, and

e. Pressurizer Pressure - Low.

The RPS satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO

The LCO requires all instrumentation performing an RPS Function to be OPERABLE. Failure of any required portion of the instrument channel renders the affected channel(s) inoperable and reduces the reliability of the affected Functions.

Actions allow maintenance (trip channel) bypass of individual channels, but the bypass activates interlocks that prevent operation with a second channel in the same Function bypassed. With one channel in each Function trip channel bypassed, this effectively places the plant in a two-out-of-three logic configuration in those Functions.

Only the Allowable Values are specified for each RPS trip Function in the LCO. Nominal trip setpoints are specified in the plant specific setpoint calculations. The nominal setpoints are selected to ensure the setpoints measured by CHANNEL FUNCTIONAL TESTS do not exceed the Allowable Value if the bistable is performing as required. Operation with a trip setpoint less conservative than the nominal trip setpoint, but within its Allowable Value, is acceptable, provided that operation and testing are consistent with the assumptions of the plant specific setpoint calculations. A channel is inoperable if its actual trip setpoint is not within its required Allowable Value. Each Allowable Value specified is more conservative than the analytical limit assumed in the safety analysis in order to account for instrument uncertainties appropriate to the trip Function. These uncertainties are defined in the "Plant Protection System Selection of Trip Setpoint Values" (Ref. 8).

The Bases for the individual Function requirements are as follows:

1. Linear Power Level - High

   This LCO requires all four channels of Linear Power Level - High to be OPERABLE in MODES 1 and 2.

   The Allowable Value is high enough to provide an operating envelope that prevents unnecessary Linear Power Level - High reactor trips during normal plant operations. The Allowable Value is low enough for the system to maintain a margin to unacceptable fuel cladding damage should a CEA ejection accident occur.

2. Logarithmic Power Level - High

   This LCO requires all four channels of Logarithmic Power Level - High to be OPERABLE in MODE 2, and in MODE 3, 4, or 5 when the RTCBs are shut and the CEA Drive System is capable of CEA withdrawal.

BASES

LCO (continued)

The MODES 3, 4, and 5 Condition is addressed in LCO 3.3.2.

The Allowable Value is high enough to provide an operating envelope that prevents unnecessary Logarithmic Power Level - High reactor trips during normal plant operations. The Allowable Value is low enough for the system to maintain a margin to unacceptable fuel cladding damage should a CEA withdrawal event occur.

The Logarithmic Power Level - High trip may be bypassed when logarithmic power is above 1E-4% to allow the reactor to be brought to power during a reactor startup. This bypass is automatically removed when logarithmic power decreases below 1E-4%. Above 1E-4%, the Linear Power Level - High and Pressurizer Pressure - High trips provide protection for reactivity transients.

The trip may be manually bypassed during physics testing pursuant to LCO 3.4.17, "RCS Loops - Test Exceptions." During this testing, the Linear Power Level - High trip and administrative controls provide the required protection.

3. Pressurizer Pressure - High

This LCO requires four channels of Pressurizer Pressure - High to be OPERABLE in MODES 1 and 2.

The Allowable Value is set below the nominal lift setting of the pressurizer code safety valves, and its operation avoids the undesirable operation of these valves during normal plant operation. In the event of a complete loss of electrical load from 100% power, this setpoint ensures the reactor trip will take place, thereby limiting further heat input to the RCS and consequent pressure rise. The pressurizer safety valves may lift to prevent overpressurization of the RCS.

4. Pressurizer Pressure - Low

This LCO requires four channels of Pressurizer Pressure - Low to be OPERABLE in MODES 1 and 2.

The Allowable Value is set low enough to prevent a reactor trip during normal plant operation and pressurizer pressure transients. However, the setpoint is high enough that with a LOCA, the reactor trip will occur soon enough to allow the ESF systems to perform as expected in the analyses and mitigate the consequences of the accident.

BASES

LCO (continued)

The trip setpoint may be manually decreased to a minimum value of 300 psia as pressurizer pressure is reduced during controlled plant shutdowns, provided the margin between the pressurizer pressure and the setpoint is maintained < 400 psia. This allows for controlled depressurization of the RCS while still maintaining an active trip setpoint until the time is reached when the trip is no longer needed to protect the plant. Since the same Pressurizer Pressure - Low bistable is also shared with the SIAS, an inadvertent SIAS actuation is also prevented. The setpoint increases automatically as pressurizer pressure increases, until the trip setpoint is reached.

The Pressurizer Pressure - Low trip and the SIAS Function may be simultaneously bypassed when RCS pressure is below 500 psia, when neither the reactor trip nor an inadvertent SIAS actuation are desirable and these Functions are no longer needed to protect the plant. The bypass is automatically removed as RCS pressure increases above 500 psia.

5. Containment Pressure - High

The LCO requires four channels of Containment Pressure - High to be OPERABLE in MODES 1 and 2.

The Allowable Value is set high enough to allow for small pressure increases in containment expected during normal operation (i.e., plant heatup) and is not indicative of an abnormal condition. It is set low enough to initiate a reactor trip when an abnormal condition is indicated.

6, 7. Steam Generator Pressure - Low

This LCO requires four channels of Steam Generator #1 Pressure - Low and Steam Generator #2 Pressure - Low to be OPERABLE in MODES 1 and 2.

This Allowable Value is sufficiently below the full load operating value for steam pressure so as not to interfere with normal plant operation, but still high enough to provide the required protection in the event of excessive steam demand. Since excessive steam demand causes the RCS to cool down, resulting in positive reactivity addition to the core, a reactor trip is required to offset that effect.

BASES

LCO (continued)

The trip setpoint may be manually decreased as steam generator pressure is reduced during controlled plant cooldown, provided the margin between steam generator pressure and the setpoint is maintained < 200 psia. This allows for controlled depressurization of the secondary system while still maintaining an active reactor trip setpoint and MSIS setpoint, until the time is reached when the setpoints are no longer needed to protect the plant. The setpoint increases automatically as steam generator pressure increases until the specified trip setpoint is reached.

8, 9. <u>Steam Generator Level – Low</u>

This LCO requires four channels of Steam Generator #1 Level - Low and Steam Generator #2 Level - Low for each steam generator to be OPERABLE in MODES 1 and 2.

The Allowable Value is sufficiently below the normal operating level for the steam generators so as not to cause a reactor trip during normal plant operations. The same bistable providing the reactor trip also initiates emergency feedwater to the affected generator via the Emergency Feedwater Actuation Signals (EFAS). The minimum setpoint is governed by EFAS requirements. The reactor trip will remove the heat source (except decay heat), thereby conserving the reactor heat sink.

This trip may be manually bypassed when cold leg temperature is below the specified limit to allow for CEA withdrawal during testing. The bypass is automatically removed when cold leg temperature reaches 200°F.

10, 11. <u>Reactor Coolant Flow – Low</u>

This LCO requires four channels of Reactor Coolant Flow, Steam Generator #1 - Low and Reactor Coolant Flow, Steam Generator #2 - Low to be OPERABLE in MODES 1 and 2. The Allowable Value is set low enough to allow for slight variations in reactor coolant flow during normal plant operations while providing the required protection. Tripping the reactor ensures that the resultant power to flow ratio provides adequate core cooling to maintain DNBR under the expected pressure conditions for this event.

BASES

LCO (continued)

The Reactor Coolant Flow - Low trip may be manually bypassed when logarithmic power is less than 1E-4%. This allows for de-energization of one or more RCPs (e.g., for plant cooldown), while maintaining the ability to keep the shutdown CEA banks withdrawn from the core if desired.

LCO 3.4.5, "RCS Loops - MODE 3," LCO 3.4.6, "RCS Loops - MODE 4," and LCO 3.4.7, "RCS Loops - MODE 5, Loops Filled," ensure adequate RCS flow rate is maintained. The bypass is automatically removed when logarithmic power increases above 1E-4%, as sensed by the wide range (logarithmic) nuclear instrumentation. When below the power range, the Reactor Coolant Flow - Low is not required for plant protection.

12. Loss of Load

This LCO requires four channels of Loss of Load trip to be OPERABLE in MODES 1 and 2.

The Steam Bypass Control System is capable of passing 45% of the full power main steam flow (45% RTP bypass capability) directly to the condenser without causing the MSSVs to lift. The Nuclear Steam Supply System is capable of absorbing a 10% step change in power when a primary to secondary system energy mismatch occurs, without causing the pressurizer safety valves to lift. This means that the plant can sustain a turbine trip without causing the pressurizer safety valves or the MSSV to lift, provided power is ≤ 55% RTP. Therefore, the Loss of Load trip may be bypassed when reactor power is ≤ 55% RTP, as sensed by the power range nuclear instrumentation. Both the bypass and bypass removal, when above 55% power, are automatically performed.

Loss of Load trip is equipment protective and not credited in the accident analysis. As such, the 55% bypass power permissive is a nominal value and does not include any instrument uncertainties.

BASES

LCO (continued)

13. Local Power Density – High

This LCO requires four channels of LPD - High to be OPERABLE.

The LCO on the CPCs ensures that the SLs are maintained during all AOOs and the consequences of accidents are acceptable.

A CPC is not considered inoperable if CEAC inputs to the CPC are inoperable. The Required Actions required in the event of CEAC channel failures ensure the CPCs are capable of performing their safety Function.

The CPC channels may be manually bypassed below 1E-4%, as sensed by the logarithmic nuclear instrumentation. This bypass is enabled manually in all four CPC channels when plant conditions do not warrant the trip protection. The bypass effectively removes the DNBR - Low and LPD - High trips from the RPS Logic circuitry. The operating bypass is automatically removed when enabling bypass conditions are no longer satisfied.

This operating bypass is required to perform a plant startup, since both CPC generated trips will be in effect whenever shutdown CEAs are inserted. It also allows system tests at low power with Pressurizer Pressure - Low or RCPs off.

During special testing pursuant to LCO 3.4.17, the CPC channels may be manually bypassed when THERMAL POWER is below 5% RTP to allow special testing without generating a reactor trip. The Linear Power Level - High trip setpoint is reduced, so as to provide protection during testing.

14. Departure from Nucleate Boiling Ratio (DNBR) – Low

This LCO requires four channels of DNBR - Low to be OPERABLE.

The LCO on the CPCs ensures that the SLs are maintained during all AOOs and the consequences of accidents are acceptable.
A CPC is not considered inoperable if CEAC inputs to the CPC are inoperable. The Required Actions required in the event of CEAC channel failures ensure the CPCs are capable of performing their safety Function.

BASES

LCO (continued)

The CPC channels may be manually bypassed below 1E-4%, as sensed by the logarithmic nuclear instrumentation. This bypass is enabled manually in all four CPC channels when plant conditions do not warrant the trip protection. The bypass effectively removes the DNBR - Low and LPD - High trips from the RPS logic circuitry. The operating bypass is automatically removed when enabling bypass conditions are no longer satisfied.

This operating bypass is required to perform a plant startup, since both CPC generated trips will be in effect whenever shutdown CEAs are inserted. It also allows system tests at low power with Pressurizer Pressure - Low or RCPs off.

During special testing pursuant to LCO 3.4.17, the CPC channels may be manually bypassed when THERMAL POWER is below 5% RTP to allow special testing without generating a reactor trip. The Linear Power Level - High trip setpoint is reduced, so as to provide protection during testing.

Interlocks/Bypasses

The LCO on bypass permissive removal channels requires that the automatic bypass removal feature of all four operating bypass channels be OPERABLE for each RPS Function with an operating bypass in the MODES addressed in the specific LCO for each Function. All four bypass removal channels must be OPERABLE to ensure that none of the four RPS channels are inadvertently bypassed.

This LCO applies to the bypass removal feature only. If the bypass enable Function is failed so as to prevent entering a bypass condition, operation may continue. In the case of the Logarithmic Power Level - High trip (Function 2), the absence of a bypass will limit maximum power to below the trip setpoint.

The interlock function Allowable Values are based upon analysis of functional requirements for the bypassed Functions. These are discussed above as part of the LCO discussion for the affected Functions.

BASES

APPLICABILITY

Most RPS trips are required to be OPERABLE in MODES 1 and 2 because the reactor is critical in these MODES. The reactor trips are designed to take the reactor subcritical, which maintains the SLs during AOOs and assists the ESFAS in providing acceptable consequences during accidents. Most trips are not required to be OPERABLE in MODES 3, 4, and 5. In MODES 3, 4, and 5, the emphasis is placed on return to power events. The reactor is protected in these MODES by ensuring adequate SDM. Exceptions to this are:

- The Logarithmic Power Level - High trip, RPS Logic RTCBs, and Manual Trip are required in MODES 3, 4, and 5, with the RTCBs closed, to provide protection for boron dilution and CEA withdrawal events.

The Logarithmic Power Level - High trip in these lower MODES is addressed in LCO 3.3.2. The Logarithmic Power Level - High trip is bypassed prior to MODE 1 entry and is not required in MODE 1. The RPS Logic in MODES 1, 2, 3, 4, and 5 is addressed in LCO 3.3.4.

ACTIONS

The most common causes of channel inoperability are outright failure or drift of the bistable or process module sufficient to exceed the tolerance allowed by the plant specific setpoint analysis. Typically, the drift is found to be small and results in a delay of actuation rather than a total loss of function. This determination is generally made during the performance of a CHANNEL FUNCTIONAL TEST when the process instrument is set up for adjustment to bring it to within specification. If the trip setpoint is less conservative than the Allowable Value in Table 3.3.1-1, the channel is declared inoperable immediately, and the appropriate Condition(s) must be entered immediately.

In the event a channel's trip setpoint is found nonconservative with respect to the Allowable Value, or the transmitter, instrument loop, signal processing electronics, or RPS bistable trip unit is found inoperable, then all affected functions provided by that channel must be declared inoperable, and the unit must enter the Condition for the particular protection Function affected.

When the number of inoperable channels in a trip Function exceeds that specified in any related Condition associated with the same trip Function, then the plant is outside the safety analysis. Therefore, LCO 3.0.3 is immediately entered if applicable in the current MODE of operation.

BASES

ACTIONS (continued)

A Note has been added to the ACTIONS. The Note has been added to clarify the application of the Completion Time rules. The Conditions of this Specification may be entered independently for each Function. The Completion Times of each inoperable Function will be tracked separately for each Function, starting from the time the Condition was entered for that Function.

A.1 and A.2

Condition A applies to the failure of a single trip channel or associated instrument channel inoperable in any RPS automatic trip Function. RPS coincidence logic is two-out-of-four.

If one RPS channel is inoperable, startup or power operation is allowed to continue, providing the inoperable channel is placed in bypass or trip in 1 hour (Required Action A.1). The 1 hour allotted to bypass or trip the channel is sufficient to allow the operator to take all appropriate actions for the failed channel and still ensures that the risk involved in operating with the failed channel is acceptable. The failed channel must be restored to OPERABLE status prior to entering MODE 2 following the next MODE 5 entry. With a channel in bypass, the coincidence logic is now in a two-out-of-three configuration.

The Completion Time of prior to entering MODE 2 following the next MODE 5 entry is based on adequate channel to channel independence, which allows a two-out-of-three channel operation since no single failure will cause or prevent a reactor trip.

B.1

Condition B applies to the failure of two channels in any RPS automatic trip Function.

Required Action B.1 provides for placing one inoperable channel in bypass and the other channel in trip within the Completion Time of 1 hour. This Completion Time is sufficient to allow the operator to take all appropriate actions for the failed channels while ensuring the risk involved in operating with the failed channels is acceptable. With one channel of protective instrumentation bypassed, the RPS is in a two-out-of-three logic; but with another channel failed, the RPS may be operating in a two-out-of-two logic. This is outside the assumptions made in the analyses and should be corrected. To correct the problem, the second channel is placed in trip. This places the RPS in a one-out-of-two logic. If any of the other OPERABLE channels receives a trip signal, the reactor will trip.

BASES

ACTIONS (continued)

One of the two inoperable channels will need to be restored to operable status prior to the next required CHANNEL FUNCTIONAL TEST, because channel surveillance testing on an OPERABLE channel requires that the OPERABLE channel be placed in bypass. However, it is not possible to bypass more than one RPS channel, and placing a second channel in trip will result in a reactor trip. Therefore, if one RPS channel is in trip and a second channel is in bypass, a third inoperable channel would place the unit in LCO 3.0.3.

<u>C.1, C.2.1, and C.2.2</u>

Condition C applies to one automatic bypass removal channel inoperable. If the inoperable bypass removal channel for any bypass channel cannot be restored to OPERABLE status within 1 hour, the associated RPS channel may be considered OPERABLE only if the bypass is not in effect. Otherwise, the affected RPS channel must be declared inoperable, as in

Condition A, and the affected automatic trip channel placed in bypass or trip. The bypass removal channel and the automatic trip channel must be repaired prior to entering MODE 2 following the next MODE 5 entry. The Bases for the Required Actions and required Completion Times are consistent with Condition A.

<u>D.1 and D.2</u>

Condition D applies to two inoperable automatic bypass removal channels. If the bypass removal channels for two operating bypasses cannot be restored to OPERABLE status within 1 hour, the associated RPS channel may be considered OPERABLE only if the bypass is not in effect. Otherwise, the affected RPS channels must be declared inoperable, as in Condition B, and the bypass either removed or one automatic trip channel placed in bypass and the other in trip within 1 hour. The restoration of one affected bypassed automatic trip channel must be completed prior to the next CHANNEL FUNCTIONAL TEST, or the plant must shut down per LCO 3.0.3 as explained in Condition B.

BASES

ACTIONS (continued)

E.1

Condition E applies if any CPC cabinet receives a high temperature alarm. There is one temperature sensor in each of the four CPC bays. Since CPC bays B and C also house CEAC calculators 1 and 2, respectively, a high temperature in either of these bays may also indicate a problem with the associated CEAC. CEAC OPERABILITY is addressed in LCO 3.3.3.

If a CPC cabinet high temperature alarm is received, it is possible for the CPC to be affected and not be completely reliable. Therefore, a CHANNEL FUNCTIONAL TEST must be performed within 12 hours. The Completion Time of 12 hours is adequate considering the low probability of undetected failure, the consequences of a single channel failure, and the time required to perform a CHANNEL FUNCTIONAL TEST.

F.1

Condition F applies if an OPERABLE CPC has three or more autorestarts in a 12 hour period.

CPCs and CEACs will attempt to autorestart if they detect a fault condition, such as a calculator malfunction or loss of power. A successful autorestart restores the calculator to operation; however, excessive autorestarts might be indicative of a calculator problem.

If a nonbypassed CPC has three or more autorestarts, it may not be completely reliable. Therefore, a CHANNEL FUNCTIONAL TEST must be performed on the CPC to ensure it is functioning properly. Based on plant operating experience, the Completion Time of 24 hours is adequate and reasonable to perform the test while still keeping the risk of operating in this condition at an acceptable level, since overt channel failure will most likely be indicated and annunciated in the control room by CPC online diagnostics.

G.1

Condition G is entered when the Required Action and associated Completion Time of Condition A, B, C, D, E, or F are not met.

BASES

ACTIONS (continued)

If the Required Actions associated with these Conditions cannot be completed within the required Completion Time, the reactor must be brought to a MODE where the Required Actions do not apply. The allowed Completion Time of 6 hours is reasonable, based on operating experience, for reaching the required MODE from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

The SRs for any particular RPS Function are found in the SR column of Table 3.3.1-1 for that Function. Most Functions are subject to CHANNEL CHECK, CHANNEL FUNCTIONAL TEST, CHANNEL CALIBRATION, and response time testing.

-----------------------------------REVIEWER'S NOTE-----------------------------------
In order for a plant to take credit for topical reports as the basis for justifying Frequencies, topical reports must be supported by an NRC staff SER that establishes the acceptability of each topical report for that unit.

<u>SR 3.3.1.1</u>

Performance of the CHANNEL CHECK once every 12 hours ensures that gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the parameter indicated on one channel to a similar parameter on other channels. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value. Significant deviations between the two instrument channels could be an indication of excessive instrument drift in one of the channels or of something even more serious. CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying that the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

Agreement criteria are determined by the plant staff based on a combination of the channel instrument uncertainties, including indication and readability. If a channel is outside the criteria, it may be an indication that the transmitter or the signal processing equipment has drifted outside its limits.

The Frequency, about once every shift, is based on operating experience that demonstrates the rarity of channel failure. Since the probability of two random failures in redundant channels in any 12 hour period is extremely low, the CHANNEL CHECK minimizes the chance of loss of protective function due to failure of redundant channels. The CHANNEL CHECK supplements less formal, but more frequent, checks of channel OPERABILITY during normal operational use of the displays associated with the LCO required channels.

BASES

SURVEILLANCE REQUIREMENTS (continued)

In the case of RPS trips with multiple inputs, such as the DNBR and LPD inputs to the CPCs, a CHANNEL CHECK must be performed on all inputs.

SR 3.3.1.2

The RCS flow rate indicated by each CPC is verified, as required by a Note, to be less than or equal to the actual RCS total flow rate every 12 hours when THERMAL POWER is ≥ 70% RTP. The 12 hours after reaching 70% RTP is for plant stabilization, data taking, and flow verification. This check (and if necessary, the adjustment of the CPC addressable constant flow coefficients) ensures that the DNBR setpoint is conservatively adjusted with respect to actual flow indications, as determined by the Core Operating Limits Supervisory System (COLSS).

SR 3.3.1.3

The CPC autorestart count is checked every 12 hours to monitor the CPC and CEAC for normal operation. If three or more autorestarts of a nonbypassed CPC occur within a 12 hour period, the CPC may not be completely reliable. Therefore, the Required Action of Condition F must be performed. The Frequency is based on operating experience that demonstrates the rarity of more than one channel failing within the same 12 hour interval.

SR 3.3.1.4

A daily calibration (heat balance) is performed when THERMAL POWER is ≥ 20%. The Linear Power Level signal and the CPC addressable constant multipliers are adjusted to make the CPC ΔT power and nuclear power calculations agree with the calorimetric calculation if the absolute difference is ≥ 2%. The value of 2% is adequate because this value is assumed in the safety analysis. These checks (and, if necessary, the adjustment of the Linear Power Level signal and the CPC addressable constant coefficients) are adequate to ensure that the accuracy of these CPC calculations is maintained within the analyzed error margins. The power level must be > 20% RTP to obtain accurate data. At lower power levels, the accuracy of calorimetric data is questionable.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The Frequency of 24 hours is based on plant operating experience and takes into account indications and alarms located in the control room to detect deviations in channel outputs. The Frequency is modified by a Note indicating this Surveillance need only be performed within 12 hours after reaching 20% RTP. The 12 hours after reaching 20% RTP is required for plant stabilization, data taking, and flow verification. The secondary calorimetric is inaccurate at lower power levels. A second Note in the SR indicates the SR may be suspended during PHYSICS TESTS. The conditional suspension of the daily calibrations under strict administrative control is necessary to allow special testing to occur.

SR 3.3.1.5

The RCS flow rate indicated by each CPC is verified to be less than or equal to the RCS total flow rate every 31 days. The Note indicates the Surveillance is performed within 12 hours after THERMAL POWER is ≥ 70% RTP. This check (and, if necessary, the adjustment of the CPC addressable flow constant coefficients) ensures that the DNBR setpoint is conservatively adjusted with respect to actual flow indications as determined by a calorimetric calculation. Operating experience has shown the specified Frequency is adequate, as instrument drift is minimal and changes in actual flow rate are minimal over core life.

SR 3.3.1.6

The three vertically mounted excore nuclear instrumentation detectors in each channel are used to determine APD for use in the DNBR and LPD calculations. Because the detectors are mounted outside the reactor vessel, a portion of the signal from each detector is from core sections not adjacent to the detector. This is termed shape annealing and is compensated for after every refueling by performing SR 3.3.1.12, which adjusts the gains of the three detector amplifiers for shape annealing. SR 3.3.1.6 ensures that the preassigned gains are still proper. Power must be > 15% because the CPCs do not use the excore generated signals for axial flux shape information at low power levels. The Note allowing 12 hours after reaching 15% RTP is required for plant stabilization and testing.

The 31 day Frequency is adequate because the demonstrated long term drift of the instrument channels is minimal.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.1.7

A CHANNEL FUNCTIONAL TEST on each channel except Loss of Load, power range neutron flux, and logarithmic power level channels is performed every 92 days to ensure the entire channel will perform its intended function when needed. The SR is modified by two Notes. Note 1 is a requirement to verify the correct CPC addressable constant values are installed in the CPCs when the CPC CHANNEL FUNCTIONAL TEST is performed. Note 2 allows the CHANNEL FUNCTIONAL TEST for the Logarithmic Power Level - High channels to be performed 2 hours after logarithmic power drops below 1E-4% and is required to be performed only if the RTCBs are closed.

In addition to power supply tests, the RPS CHANNEL FUNCTIONAL TEST consists of three overlapping tests as described in Reference 9. These tests verify that the RPS is capable of performing its intended function, from bistable input through the RTCBs. They include:

Bistable Tests

A test signal is superimposed on the input in one channel at a time to verify that the bistable trips within the specified tolerance around the setpoint. This is done with the affected RPS channel trip channel bypassed. Any setpoint adjustment shall be consistent with the assumptions of the current plant specific setpoint analysis.

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the interval between surveillance interval extension analysis. The requirements for this review are outlined in Reference [10].

Matrix Logic Tests

Matrix Logic tests are addressed in LCO 3.3.4. This test is performed one matrix at a time. It verifies that a coincidence in the two input channels for each Function removes power from the matrix relays. During testing, power is applied to the matrix relay test coils and prevents the matrix relay contacts from assuming their de-energized state. This test will detect any short circuits around the bistable contacts in the coincidence logic, such as may be caused by faulty bistable relay or trip channel bypass contacts.

BASES

SURVEILLANCE REQUIREMENTS (continued)

Trip Path Tests

Trip path (Initiation Logic) tests are addressed in LCO 3.3.4. These tests are similar to the Matrix Logic tests, except that test power is withheld from one matrix relay at a time, allowing the initiation circuit to de-energize, thereby opening the affected set of RTCBs. The RTCBs must then be closed prior to testing the other three initiation circuits, or a reactor trip may result.

The Frequency of 92 days is based on the reliability analysis presented in topical report CEN-327, "RPS/ESFAS Extended Test Interval Evaluation" (Ref. 10).

The CPC and CEAC channels and excore nuclear instrumentation channels are tested separately.

The excore channels use preassigned test signals to verify proper channel alignment. The excore logarithmic channel test signal is inserted into the preamplifier input, so as to test the first active element downstream of the detector.

The power range excore test signal is inserted at the drawer input, since there is no preamplifier.

The quarterly CPC CHANNEL FUNCTIONAL TEST is performed using software. This software includes preassigned addressable constant values that may differ from the current values. Provisions are made to store the addressable constant values on a computer disk prior to testing and to reload them after testing. A Note is added to the Surveillance Requirements to verify that the CPC CHANNEL FUNCTIONAL TEST includes the correct values of addressable constants. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.1.8

A Note indicates that neutron detectors are excluded from CHANNEL CALIBRATION. A CHANNEL CALIBRATION of the power range neutron flux channels every 92 days ensures that the channels are reading accurately and within tolerance (Ref. 10). The Surveillance verifies that the channel responds to a measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drift between successive calibrations to ensure that the channel remains operational between successive tests. CHANNEL CALIBRATIONS must be performed consistent with the plant specific setpoint analysis.

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the interval between surveillance interval extension analysis. The requirements for this review are outlined in Reference 10. Operating experience has shown this Frequency to be satisfactory. The detectors are excluded from CHANNEL CALIBRATION because they are passive devices with minimal drift and because of the difficulty of simulating a meaningful signal. Slow changes in detector sensitivity are compensated for by performing the daily calorimetric calibration (SR 3.3.1.4) and the monthly linear subchannel gain check (SR 3.3.1.6). In addition, the associated control room indications are monitored by the operators.

[SR 3.3.1.9

The characteristics and Bases for this Surveillance are as described for SR 3.3.1.7. This Surveillance differs from SR 3.3.1.7 only in that the CHANNEL FUNCTIONAL TEST on the Loss of Load functional unit is only required above 55% RTP. When above 55% and the trip is in effect, the CHANNEL FUNCTIONAL TEST will ensure the channel will perform its equipment protective function if needed. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions. The Note allowing 2 hours after reaching 55% RTP is necessary for Surveillance performance. This Surveillance cannot be performed below 55% RTP, since the trip is bypassed.]

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.1.10

SR 3.3.1.10 is the performance of a CHANNEL CALIBRATION every [18] months.

CHANNEL CALIBRATION is a complete check of the instrument channel including the sensor. The Surveillance verifies that the channel responds to a measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drift between successive calibrations to ensure that the channel remains operational between successive tests. CHANNEL CALIBRATIONS must be performed consistent with the plant specific setpoint analysis.

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the surveillance interval extension analysis. The requirements for this review are outlined in Reference [10].

The Frequency is based upon the assumption of an [18] month calibration interval for the determination of the magnitude of equipment drift in the setpoint analysis as well as operating experience and consistency with the typical [18] month fuel cycle.

The Surveillance is modified by a Note to indicate that the neutron detectors are excluded from CHANNEL CALIBRATION because they are passive devices with minimal drift and because of the difficulty of simulating a meaningful signal. Slow changes in detector sensitivity are compensated for by performing the daily calorimetric calibration (SR 3.3.1.4) and the monthly linear subchannel gain check (SR 3.3.1.6).

SR 3.3.1.11

Every [18] months, a CHANNEL FUNCTIONAL TEST is performed on the CPCs. The CHANNEL FUNCTIONAL TEST shall include the injection of a signal as close to the sensors as practicable to verify OPERABILITY including alarm and trip Functions. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The basis for the [18] month Frequency is that the CPCs perform a continuous self monitoring function that eliminates the need for frequent CHANNEL FUNCTIONAL TESTS. This CHANNEL FUNCTIONAL TEST essentially validates the self monitoring function and checks for a small set of failure modes that are undetectable by the self monitoring function. Operating experience has shown that undetected CPC or CEAC failures do not occur in any given [18] month interval.

SR 3.3.1.12

The three excore detectors used by each CPC channel for axial flux distribution information are far enough from the core to be exposed to flux from all heights in the core, although it is desired that they only read their particular level. The CPCs adjust for this flux overlap by using the predetermined shape annealing matrix elements in the CPC software.

After refueling, it is necessary to re-establish or verify the shape annealing matrix elements for the excore detectors based on more accurate incore detector readings. This is necessary because refueling could possibly produce a significant change in the shape annealing matrix coefficients.

Incore detectors are inaccurate at low power levels. THERMAL POWER should be significant but < 70% to perform an accurate axial shape calculation used to derive the shape annealing matrix elements.

By restricting power to ≤ 70% until shape annealing matrix elements are verified, excessive local power peaks within the fuel are avoided. Operating experience has shown this Frequency to be acceptable.

SR 3.3.1.13

SR 3.3.1.13 is a CHANNEL FUNCTIONAL TEST similar to SR 3.3.1.7, except SR 3.3.1.13 is applicable only to bypass functions and is performed once within 92 days prior to each startup. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical

BASES

SURVEILLANCE REQUIREMENTS (continued)

Specifications tests at least once per refueling interval with applicable extensions. Proper operation of bypass permissives is critical during plant startup because the bypasses must be in place to allow startup operation and must be removed at the appropriate points during power ascent to enable certain reactor trips. Consequently, the appropriate time to verify bypass removal function OPERABILITY is just prior to startup. The allowance to conduct this Surveillance within 92 days of startup is based on the reliability analysis presented in topical report CEN-327, "RPS/ESFAS Extended Test Interval Evaluation" (Ref. 10). Once the operating bypasses are removed, the bypasses must not fail in such a way that the associated trip Function gets inadvertently bypassed. This feature is verified by the trip Function CHANNEL FUNCTIONAL TEST, SR 3.3.1.7 or SR 3.3.1.9. Therefore, further testing of the bypass function after startup is unnecessary.

SR 3.3.1.14

This SR ensures that the RPS RESPONSE TIMES are verified to be less than or equal to the maximum values assumed in the safety analysis. Individual component response times are not modeled in the analyses. The analyses model the overall or total elapsed time, from the point at which the parameter exceeds the trip setpoint value at the sensor to the point at which the RTCBs open. Response times are conducted on an [18] month STAGGERED TEST BASIS. This results in the interval between successive surveillances of a given channel of n x 18 months, where n is the number of channels in the function. The Frequency of [18] months is based upon operating experience, which has shown that random failures of instrumentation components causing serious response time degradation, but not channel failure, are infrequent occurrences. Also, response times cannot be determined at power, since equipment operation is required. Testing may be performed in one measurement or in overlapping segments, with verification that all components are tested.

-----------------------------------REVIEWER'S NOTE-----------------------------------
Applicable portions of the following TS Bases are applicable to plants adopting CEOG Topical Report CE NPSD-1167-1, "Elimination of Pressure Sensor Response Time Testing Requirements."

BASES

SURVEILLANCE REQUIREMENTS (continued)

Response time may be verified by any series of sequential, overlapping or total channel measurements, including allocated sensor response time, such that the response time is verified. Allocations for sensor response times may be obtained from records of test results, vendor test data, or vendor engineering specifications. Topical Report CE NPSD-1167-A, "Elimination of Pressure Sensor Response Time Testing Requirements," (Ref. 11) provides the basis and methodology for using allocated sensor response times in the overall verification of the channel response time for specific sensors identified in the Topical Report. Response time verification for other sensor types must be demonstrated by test. The allocation of sensor response times must be verified prior to placing a new component in operation and reverified after maintenance that may adversely affect the sensor response time.

A Note is added to indicate that the neutron detectors are excluded from RPS RESPONSE TIME testing because they are passive devices with minimal drift and because of the difficulty of simulating a meaningful signal. Slow changes in detector sensitivity are compensated for by performing the daily calorimetric calibration (SR 3.3.1.4).

REFERENCES

1. Regulatory Guide 1.105, Revision 3, "Setpoints for Safety-Related Instrumentation."

2. 10 CFR 50, Appendix A, GDC 21.

3. 10 CFR 100.

4. NRC Safety Evaluation Report.

5. IEEE Standard 279-1971, April 5, 1972.

6. FSAR, Chapter [14].

7. 10 CFR 50.49.

8. "Plant Protection System Selection of Trip Setpoint Values."

9. FSAR, Section [7.2].

10. CEN-327, June 2, 1986, including Supplement 1, March 3, 1989.

11. CEOG Topical Report CE NPSD-1167-A, "Elimination of Pressure Sensor Response Time Testing Requirements."

B 3.3 INSTRUMENTATION

B 3.3.2 Reactor Protective System (RPS) Instrumentation - Shutdown (Digital)

BASES

BACKGROUND

The RPS initiates a reactor trip to protect against violating the core fuel design limits and reactor coolant pressure boundary (RCPB) integrity during anticipated operational occurrences (AOOs). By tripping the reactor, the RPS also assists the Engineered Safety Features systems in mitigating accidents.

The protection and monitoring systems have been designed to ensure safe operation of the reactor. This is achieved by specifying limiting safety system settings (LSSS) in terms of parameters directly monitored by the RPS, as well as LCOs on other reactor system parameters and equipment performance.

The LSSS, defined in this Specification as the Allowable Value, in conjunction with the LCOs, establish the threshold for protective system action to prevent exceeding acceptable limits during Design Basis Accidents (DBAs).

During AOOs, which are those events expected to occur one or more times during the plant life, the acceptable limits are:

- The departure from nucleate boiling ratio shall be maintained above the Safety Limit (SL) value to prevent departure from nucleate boiling,
- Fuel centerline melting shall not occur, and
- The Reactor Coolant System pressure SL of 2750 psia shall not be exceeded.

Maintaining the parameters within the above values ensures that the offsite dose will be within the 10 CFR 50 (Ref. 1) and 10 CFR 100 (Ref. 2) criteria during AOOs.

Accidents are events that are analyzed even though they are not expected to occur during the plant life. The acceptable limit during accidents is that the offsite dose shall be maintained within an acceptable fraction of 10 CFR 100 (Ref. 2) limits. Different accident categories allow a different fraction of these limits based on probability of occurrence. Meeting the acceptable dose limit for an accident category is considered having acceptable consequences for that event.

BASES

BACKGROUND (continued)

The RPS is segmented into four interconnected modules. These modules are:

- Measurement channels,
- Bistable trip units,
- RPS Logic, and
- Reactor trip circuit breakers (RTCBs).

This LCO applies only to the Logarithmic Power Level - High trip in MODES 3, 4, and 5 with the RTCBs closed. In MODES 1 and 2, this trip Function is addressed in LCO 3.3.1, "Reactor Protective System (RPS) Instrumentation - Operating." LCO 3.3.13, "[Logarithmic] Power Monitoring Channels," applies when the RTCBs are open. In the case of LCO 3.3.13, the logarithmic channels are required for monitoring neutron flux, although the trip Function is not required.

Measurement Channels and Bistable Trip Units

The measurement channels providing input to the Logarithmic Power Level - High trip consist of the four logarithmic nuclear instrumentation channels detecting neutron flux leakage from the reactor vessel. Other aspects of the Logarithmic Power Level - High trip are similar to the other measurement channels and bistables. These are addressed in the Background section of LCO 3.3.1.

Functional testing of the entire RPS, from bistable input through the opening of individual sets of RTCBs, can be performed either at power or shutdown and is normally performed on a quarterly basis. Nuclear instrumentation can be similarly tested. FSAR, Section [7.2] (Ref. 3), provides more detail on RPS testing.

APPLICABLE SAFETY ANALYSES

The RPS functions to maintain the SLs during AOOs and mitigates the consequence of DBAs in all MODES in which the RTCBs are closed.

Each of the analyzed transients and accidents can be detected by one or more RPS Functions. Functions not specifically credited in the accident analysis were qualitatively credited in the safety analysis and the NRC staff approved licensing basis for the plant. Noncredited Functions include the Loss of Load. The Loss of Load trip is purely equipment protective, and its use minimizes the potential for equipment damage.

BASES

APPLICABLE SAFETY ANALYSES (continued)

The Logarithmic Power Level - High trip protects the integrity of the fuel cladding and helps protect the RCPB in the event of an unplanned criticality from a shutdown condition.

In MODES 2, 3, 4, and 5, with the RTCBs closed, and the Control Element Assembly (CEA) Drive System capable of CEA withdrawal, protection is required for CEA withdrawal events originating when logarithmic power is < 1E-4%. For events originating above this power level, other trips provide adequate protection.

MODES 3, 4, and 5, with the RTCBs closed, are addressed in this LCO. MODE 2 is addressed in LCO 3.3.1.

In MODES 3, 4, or 5, with the RTCBs open or the CEAs not capable of withdrawal, the Logarithmic Power Level - High trip does not have to be OPERABLE. However, the indication and alarm portion of two logarithmic channels must be OPERABLE to ensure proper indication of neutron population and to indicate a boron dilution event. The indication and alarm functions are addressed in LCO 3.3.13.

The RPS satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

The LCO requires the Logarithmic Power Level - High RPS Function to be OPERABLE. Failure of any required portion of the instrument channel renders the affected channel(s) inoperable and reduces the reliability of the affected Function.

Actions allow maintenance (trip channel) bypass of individual channels, but the bypass activates interlocks that prevent operation with a second channel in the same Function bypassed. With one channel in each Function trip channel bypassed, this effectively places the plant in a two-out-of-three logic configuration in those Functions. Plants are restricted to 48 hours in a trip channel bypass condition before either restoring the function to four channel operation (two-out-of-four logic) or placing the channel in trip (one-out-of-three logic).

This LCO requires all four channels of the Logarithmic Power Level - High to be OPERABLE in MODE 2, and in MODE 3, 4, or 5 when the RTCBs are closed and the CEA Drive System is capable of CEA withdrawal.

BASES

LCO (continued)

The Allowable Value specified in SR 3.3.2.4 is high enough to provide an operating envelope that prevents unnecessary Logarithmic Power Level - High reactor trips during normal plant operations. The Allowable Value is low enough for the system to maintain a safety margin for unacceptable fuel cladding damage should a CEA withdrawal event occur.

The Logarithmic Power Level - High trip may be bypassed when logarithmic power is above 1E-4% to allow the reactor to be brought to power during a reactor startup. This bypass is automatically removed when logarithmic power decreases below 1E-4%. Above 1E-4%, the Linear Power Level - High and Pressurizer Pressure - High trips provide protection for reactivity transients.

The trip may be manually bypassed during physics testing pursuant to LCO 3.4.17, "RCS Loops - Test Exceptions." During this testing, the Linear Power Level - High trip and administrative controls provide the required protection.

APPLICABILITY

Most RPS trips are required to be OPERABLE in MODES 1 and 2 because the reactor is critical in these MODES. The trips are designed to take the reactor subcritical, which maintains the SLs during AOOs and assists the Engineered Safety Features Actuation System (ESFAS) in providing acceptable consequences during accidents. Most trips are not required to be OPERABLE in MODES 3, 4, and 5. In MODES 3, 4, and 5, the emphasis is placed on return to power events. The reactor is protected in these MODES by ensuring adequate SDM. Exceptions to this are:

- The Logarithmic Power Level - High trip, RPS Logic RTCBs, and Manual Trip are required in MODES 3, 4, and 5, with the RTCBs closed, to provide protection for boron dilution and CEA withdrawal events. The Logarithmic Power Level - High trip in these lower MODES is addressed in this LCO. The RPS Logic in MODES 1, 2, 3, 4, and 5 is addressed in LCO 3.3.4, "Reactor Protective System (RPS) Logic and Trip Initiation."

The Applicability is modified by a Note that allows the trip to be bypassed when logarithmic power is > 1E-4%, and the bypass is automatically removed when logarithmic power is ≤ 1E-4%.

BASES

ACTIONS

The most common causes of channel inoperability are outright failure or drift of the bistable or process module sufficient to exceed the tolerance allowed by the plant specific setpoint analysis. Typically, the drift is found to be small and results in a delay of actuation rather than a total loss of function. This determination is generally made during the performance of a CHANNEL FUNCTIONAL TEST when the process instrument is set up for adjustment to bring it to within specification. If the trip setpoint is less conservative than the Allowable Value stated in the LCO, the channel is declared inoperable immediately, and the appropriate Condition(s) must be entered immediately.

In the event a channel's trip setpoint is found nonconservative with respect to the Allowable Value, or the excore logarithmic power channel or RPS bistable trip unit is found inoperable, then all affected Functions provided by that channel must be declared inoperable and the unit must enter the Condition for the particular protection Function affected.

When the number of inoperable channels in a trip Function exceeds that specified in any related Condition associated with the same trip Function, then the plant is outside the safety analysis. Therefore, LCO 3.0.3 is immediately entered, if applicable in the current MODE of operation.

A.1, and A.2

Condition A applies to the failure of a single Logarithmic Power Level - High trip channel or associated instrument channel.

The Logarithmic Power Level - High coincidence logic is two-out-of-four. If one channel is inoperable, operation in MODES 3, 4, and 5 is allowed to continue, providing the inoperable channel is placed in bypass or trip in 1 hour (Required Action A.1).

The 1 hour allotted to bypass or trip the channel is sufficient to allow the operator to take all appropriate actions for the failed channel while ensuring that the risk involved in operating with the failed channel is acceptable.

The failed channel must be restored to OPERABLE status prior to entering MODE 2 following the next MODE 5 entry. With a channel bypassed, the coincidence logic is now in a two-out-of-three configuration. The Completion Time is based on adequate channel to channel independence, which allows a two-out-of-three channel operation since no single failure will cause or prevent a reactor trip.

BASES

ACTIONS (continued)

B.1

Condition B applies to the failure of two Logarithmic Power Level - High trip channels or associated instrument channels. Required Action B.1 provides for placing one inoperable channel in bypass and the other channel in trip within the Completion Time of 1 hour. This Completion Time is sufficient to allow the operator to take all appropriate actions for the failed channels and still ensures the risk involved in operating with the failed channels is acceptable. With one channel of protective instrumentation bypassed, the RPS is in a two-out-of-three logic; but with another channel failed, the RPS may be operating in a two-out-of-two logic. This is outside the assumptions made in the analyses and should be corrected. To correct the problem, the second channel is placed in trip. This places the RPS in a one-out-of-two logic. If any of the other OPERABLE channels receives a trip signal, the reactor will trip.

One of the two inoperable channels will need to be restored to OPERABLE status prior to the next required CHANNEL FUNCTIONAL TEST because channel surveillance testing on an OPERABLE channel requires that the OPERABLE channel be placed in bypass. However, it is not possible to bypass more than one RPS channel, and placing a second channel in trip will result in a reactor trip. Therefore, if one RPS channel is in trip and a second channel is in bypass, a third inoperable channel would place the unit in LCO 3.0.3.

C.1, C.2.1, and C.2.2

Condition C applies to one automatic bypass removal channel inoperable. If the bypass removal channel for the high logarithmic power level operating bypass cannot be restored to OPERABLE status within 1 hour, the associated RPS channel may be considered OPERABLE only if the bypass is not in effect. Otherwise, the affected RPS channel must be declared inoperable, as in Condition A, and the bypass either removed or the affected automatic channel placed in trip or bypass. Both the bypass removal channel and the associated automatic trip channel must be repaired prior to entering MODE 2 following the next MODE 5 entry. The Bases for the Required Actions and required Completion Times are consistent with Condition A.

BASES

ACTIONS (continued)

D.1 and D.2

Condition D applies to two inoperable automatic bypass removal channels. If the bypass removal channels for two operating bypasses cannot be restored to OPERABLE status within 1 hour, the associated RPS channel may be considered OPERABLE only if the bypass is not in effect. Otherwise, the affected RPS channels must be declared inoperable, as in Condition B, and the bypass either removed or one automatic trip channel placed in bypass and the other in trip within 1 hour. The restoration of one affected bypassed automatic trip channel must be completed prior to the next CHANNEL FUNCTIONAL TEST or the plant must shut down per LCO 3.0.3, as explained in Condition B. Completion Times are consistent with Condition B.

E.1

Condition E is entered when the Required Actions and associated Completion Times of Condition A, B, C, or D are not met.

If Required Actions associated with these Conditions cannot be completed within the required Completion Time, all RTCBs must be opened, placing the plant in a condition where the logarithmic power trip channels are not required to be OPERABLE. A Completion Time of 1 hour is a reasonable time to perform the Required Action, which maintains the risk at an acceptable level while having one or two channels inoperable.

SURVEILLANCE REQUIREMENTS

The SRs for the Logarithmic Power Level - High trip are an extension of those listed in LCO 3.3.1, listed here because of their Applicability in these MODES.

-----------------------------------REVIEWER'S NOTE-----------------------------------
In order for a unit to take credit for topical reports as the basis for justifying Frequencies, topical reports must be supported by an NRC staff Safety Evaluation Report that establishes the acceptability of each topical report for that unit (Ref. 5).

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.2.1

SR 3.3.2.1 is the performance of a CHANNEL CHECK of each logarithmic power channel. This SR is identical to SR 3.3.1.1. Only the Applicability differs.

Performance of the CHANNEL CHECK once every 12 hours ensures that gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the parameter indicated on one channel to a similar parameter on another channel. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value. Significant deviations between the two instrument channels could be an indication of excessive instrument drift in one of the channels or of something even more serious. CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying that the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

Agreement criteria are determined by the plant staff based on a combination of the channel instrument uncertainties, including indication and readability. If a channel is outside the criteria, it may be an indication that the sensor or the signal processing equipment has drifted outside its limits.

The Frequency, about once every shift, is based on operating experience that demonstrates the rarity of channel failure. Since the probability of two random failures in redundant channels in any 12 hour period is extremely low, the CHANNEL CHECK minimizes the chance of loss of protective function due to failure of redundant channels. The CHANNEL CHECK supplements less formal, but more frequent, checks of channel OPERABILITY during normal operational use of the displays associated with the LCO required channels.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.2.2

A CHANNEL FUNCTIONAL TEST on each channel, except Loss of Load and power range neutron flux, is performed every 92 days to ensure the entire channel will perform its intended function when needed. This SR is identical to SR 3.3.1.7. Only the Applicability differs. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

In addition to power supply tests, the RPS CHANNEL FUNCTIONAL TEST consists of three overlapping tests as described in the FSAR, Section [7.2] (Ref. 3). These tests verify that the RPS is capable of performing its intended function, from bistable input through the RTCBs. They include:

Bistable Tests

A test signal is superimposed on the input in one channel at a time to verify that the bistable trips within the specified tolerance around the setpoint. This is done with the affected RPS channel trip channel bypassed. Any setpoint adjustment shall be consistent with the assumptions of the current plant specific setpoint analysis.

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the surveillance interval extension analysis. The requirements for this review are outlined in Reference [6].

Matrix Logic Tests

Matrix Logic Tests are addressed in LCO 3.3.4. This test is performed one matrix at a time. It verifies that a coincidence in the two input channels for each Function removes power from the matrix relays. During testing, power is applied to the matrix relay test coils and prevents the matrix relay contacts from assuming their de-energized state. This test will detect any short circuits around the bistable contacts in the coincidence logic, such as may be caused by faulty bistable relay or trip channel bypass contacts.

BASES

SURVEILLANCE REQUIREMENTS (continued)

Trip Path Test

Trip path (Initiation Logic) tests are addressed in LCO 3.3.4. These tests are similar to the Matrix Logic tests except that test power is withheld from one matrix relay at a time, allowing the initiation circuit to de-energize, opening the affected set of RTCBs. The RTCBs must then be closed prior to testing the other three initiation circuits, or a reactor trip may result.

The Frequency of 92 days is based on the reliability analysis presented in topical report CEN-327, "RPS/ESFAS Extended Test Interval Evaluation" (Ref. 6). The excore channels use preassigned test signals to verify proper channel alignment. The excore logarithmic channel test signal is inserted into the preamplifier input, so as to test the first active element downstream of the detector.

SR 3.3.2.3

SR 3.3.2.3 is a CHANNEL FUNCTIONAL TEST similar to SR 3.3.2.2, except SR 3.3.2.3 is applicable only to bypass functions and is performed once within 92 days prior to each startup. This SR is identical to SR 3.3.1.13. Only the Applicability differs. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

Proper operation of bypass permissives is critical during plant startup because the bypasses must be in place to allow startup operation and must be removed at the appropriate points during power ascent to enable certain reactor trips. Consequently, the appropriate time to verify bypass removal function OPERABILITY is just prior to startup. The allowance to conduct this Surveillance within 92 days of startup is based on the reliability analysis presented in topical report CEN-327, "RPS/ESFAS Extended Test Interval Evaluation" (Ref. 6). Once the operating bypasses are removed, the bypasses must not fail in such a way that the associated trip Function gets inadvertently bypassed. This feature is verified by the trip Function CHANNEL FUNCTIONAL TEST, SR 3.3.2.2. Therefore, further testing of the bypass function after startup is unnecessary.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.2.4

SR 3.3.2.4 is the performance of a CHANNEL CALIBRATION every 18 months. This SR is identical to SR 3.3.1.10. Only the Applicability differs.

CHANNEL CALIBRATION is a complete check of the instrument channel excluding the sensor. The Surveillance verifies that the channel responds to a measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drift between successive calibrations to ensure that the channel remains operational between successive tests. CHANNEL CALIBRATIONS must be performed consistent with the plant specific setpoint analysis.

Only the Allowable Values are specified for this RPS trip Function. Nominal trip setpoints are specified in the plant specific setpoint calculations. The nominal setpoint is selected to ensure the setpoint measured by CHANNEL FUNCTIONAL TESTS does not exceed the Allowable Value if the bistable is performing as required. Operation with a trip setpoint less conservative than the nominal trip setpoint, but within its Allowable Value, is acceptable provided that operation and testing are consistent with the assumptions of the plant specific setpoint calculations. Each Allowable Value specified is more conservative than the analytical limit assumed in the safety analysis in order to account for instrument uncertainties appropriate to the trip Function. These uncertainties are defined in the "Plant Protection System Selection of Trip Setpoint Values" (Ref. 4). A channel is inoperable if its actual trip setpoint is not within its required Allowable Value.

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the surveillance interval extension analysis. The requirements for this review are outlined in Reference [3].

The Frequency is based upon the assumption of an [18] month calibration interval for the determination of the magnitude of equipment drift in the setpoint analysis and includes operating experience and consistency with the typical [18] month fuel cycle.

The Surveillance is modified by a Note to indicate that the neutron detectors are excluded from CHANNEL CALIBRATION because they are passive devices with minimal drift and because of the difficulty of simulating a meaningful signal. Slow changes in detector sensitivity are compensated for by performing the daily calorimetric calibration (SR 3.3.1.4).

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.2.5

This SR ensures that the RPS RESPONSE TIMES are verified to be less than or equal to the maximum values assumed in the safety analysis. Individual component response times are not modeled in the analyses. The analyses model the overall or total elapsed time, from the point at which the parameter exceeds the trip setpoint value at the sensor to the point at which the RTCBs open. Response times are conducted on an [18] month STAGGERED TEST BASIS. This results in the interval between successive tests of a given channel of n x 18 months, where n is the number of channels in the Function. The [18] month Frequency is based upon operating experience, which has shown that random failures of instrumentation components causing serious response time degradation, but not channel failure, are infrequent occurrences. Also, response times cannot be determined at power, since equipment operation is required. Testing may be performed in one measurement or in overlapping segments, with verification that all components are tested.

REFERENCES

1. 10 CFR 50.
2. 10 CFR 100.
3. FSAR, Section [7.2].
4. "Plant Protection System Selection of Trip Setpoint Values."
5. NRC Safety Evaluation Report.
6. CEN-327, June 2, 1986, including Supplement 1, March 3, 1989.

B 3.3 INSTRUMENTATION

B 3.3.3 Control Element Assembly Calculators (CEACs) (Digital)

BASES

BACKGROUND

The Reactor Protective System (RPS) initiates a reactor trip to protect against violating the core specified acceptable fuel design limits (SAFDLs) and breaching the reactor coolant pressure boundary (RCPB) during anticipated operational occurrences (AOOs). By tripping the reactor, the RPS also assists the Engineered Safety Features systems in mitigating accidents.

The protection and monitoring systems have been designed to ensure safe operation of the reactor. This is achieved by specifying limiting safety system settings (LSSS) in terms of parameters directly monitored by the RPS, as well as LCOs on other reactor system parameters and equipment performance.

The LSSS (defined in this Specification as the Allowable Value), in conjunction with the LCOs, establish the thresholds for protective system action to prevent exceeding acceptable limits during Design Basis Accidents.

During AOOs, which are those events expected to occur one or more times during the plant life, the acceptable limits are:

- The departure from nucleate boiling ratio (DNBR) shall be maintained above the Safety Limit (SL) value to prevent departure from nucleate boiling,
- Fuel centerline melting shall not occur, and
- The Reactor Coolant System pressure SL of 2750 psia shall not be exceeded.

Maintaining the parameters within the above values ensures that the offsite dose will be within the 10 CFR 50 (Ref. 1) and 10 CFR 100 (Ref. 2) criteria during AOOs.

Accidents are events that are analyzed even though they are not expected to occur during the plant life. The acceptable limit during accidents is that the offsite dose shall be maintained within an acceptable fraction of 10 CFR 100 (Ref. 2) limits. Different accident categories allow a different fraction of these limits based on probability of occurrence. Meeting the acceptable dose limit for an accident category is considered having acceptable consequences for that event.

BASES

BACKGROUND (continued)

The RPS is segmented into four interconnected modules. These modules are:

- Measurement channels,
- Bistable trip units,
- RPS Logic, and
- Reactor trip circuit breakers (RTCBs).

This LCO addresses the CEACs. LCO 3.3.1, "Reactor Protective System (RPS) Instrumentation - Operating," provides a description of this equipment in the RPS.

The excore nuclear instrumentation, the core protection calculators (CPCs), and the CEACs are considered components in the measurement channels of the Linear Power Level - High, Logarithmic Power Level - High, DNBR - Low, and Local Power Density (LPD) - High trips. The CEACs are addressed by this Specification.

All four CPCs receive control element assembly (CEA) deviation penalty factors from each CEAC and use the larger of the power factors from the two CEACs in the calculation of DNBR and LPD. CPCs are further described in the Background section of LCO 3.3.1.

The CEACs perform the calculations required to determine the position of CEAs within their subgroups for the CPCs. Two independent CEACs compare the position of each CEA to its subgroup position. If a deviation is detected by either CEAC, an annunciator sounds and appropriate "penalty factors" are transmitted to all CPCs. These penalty factors conservatively adjust the effective operating margins to the DNBR - Low and LPD - High trips. Each CEAC also drives a single cathode ray tube (CRT), which is switchable between CEACs. The CRT displays individual CEA positions and current values of the penalty factors from the selected CEAC.

Each CEA has two separate reed switch assemblies mounted outside the RCPB. Each of the two CEACs receives CEA position input from one of the two reed switch position transmitters on each CEA, so that the position of all CEAs is independently monitored by both CEACs.

BASES

BACKGROUND (continued)

Functional testing of the entire RPS, from bistable input through the opening of individual sets of RTCBs, can be performed either at power or shutdown and is normally performed on a quarterly basis. Nuclear instrumentation, the CPCs, and the CEACs can be similarly tested. FSAR, Section [7.2] (Ref. 3), provides more detail on RPS testing. Process transmitter calibration is normally performed on a refueling basis.

APPLICABLE SAFETY ANALYSES

Each of the analyzed transients and accidents can be detected by one or more RPS Functions.

The effect of any misoperated CEA within a subgroup on the core power distribution is assessed by the CEACs, and an appropriately augmented power distribution penalty factor will be supplied as input to the CPCs. As the reactor core responds to the reactivity changes caused by the misoperated CEA and the ensuing reactor coolant and doppler feedback effects, the CPCs will initiate a DNBR - Low or LPD - High trip signal if SAFDLs are approached. Each CPC also directly monitors one "target CEA" from each subgroup and uses this information to account for excessive radial peaking factors for events involving CEA groups out of sequence and subgroup deviations within a group, without the need for CEACs.

Therefore, although the CEACs do not provide a direct reactor trip Function, their input to the CPCs is taken credit for in the CEA misoperation analysis.

The CEACs satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

This LCO on the CEACs ensures that the CPCs are either informed of individual CEA position within each subgroup, using one or both CEACs, or that appropriate conservatism is included in the CPC calculations to account for anticipated CEA deviations. Each CEAC provides an identical input into all four CPC channels. Each CPC uses the higher of the two CEAC transmitted CEA deviation penalty factors. Thus, only one OPERABLE CEAC is required to provide CEA deviation protection. This LCO requires both CEACs to be OPERABLE so that no single CEAC failure can prevent a required reactor trip from occurring.

BASES

APPLICABILITY

Most RPS trips are required to be OPERABLE in MODES 1 and 2 because the reactor is critical in these MODES. The trips are designed to take the reactor subcritical, which maintains the SLs during AOOs and assists the Engineered Safety Features Actuation System in providing acceptable consequences during accidents. Most trips are not required to be OPERABLE in MODES 3, 4, and 5. In MODES 3, 4, and 5, the emphasis is placed on return to power events. The reactor is protected in these MODES by ensuring adequate SDM.

Because CEACs provide the inputs to the DNBR - Low and LPD - High trips, they are required to be OPERABLE in the same MODES as those trips for the same reasons.

ACTIONS

A.1 and A.2

Condition A applies to the failure of a single CEAC channel. There are only two CEACs, each providing CEA deviation input into all four CPC channels. The CEACs include complex diagnostic software, making it unlikely that a CEAC will fail without informing the CPCs of its failed status. With one failed CEAC, the CPC will receive CEA deviation penalty factors from the remaining OPERABLE CEAC. If the second CEAC should fail (Condition B), the CPC will use large preassigned penalty factors. The specific Required Actions allowed are as follows:

With one CEAC inoperable, the second CEAC still provides a comprehensive set of comparison checks on individual CEAs within subgroups, as well as outputs to all CPCs, CEA deviation alarms, and position indication for display. Verification every 4 hours that each CEA is within 7 inches of the other CEAs in its group provides a check on the position of all CEAs and provides verification of the proper operation of the remaining CEAC. An OPERABLE CEAC will not generate penalty factors until deviations of > 7 inches within a subgroup are encountered.

The Completion Time of once per 4 hours is adequate based on operating experience, considering the low probability of an undetected CEA deviation coincident with an undetected failure in the remaining CEAC within this limited time frame.

As long as Required Action A.1 is accomplished as specified, the inoperable CEAC can be restored to OPERABLE status within 7 days. The Completion Time of 7 days is adequate for most repairs, while minimizing risk, considering that dropped CEAs are detectable by the redundant CEAC, and other LCOs specify Required Actions necessary to maintain DNBR and LPD margin.

BASES

ACTIONS (continued)

B.1, B.2, B.3, B.4, and B.5

Condition B applies if the Required Action and associated Completion Time of Required Action A are not met, or if both CEACs are inoperable. Actions associated with this Condition involve disabling the Control Element Drive Mechanism Control System (CEDMCS), while providing increased assurance that CEA deviations are not occurring and informing all OPERABLE CPC channels, via a software flag, that both CEACs are failed. This will ensure that the large penalty factor associated with two CEAC failures will be applied to CPC calculations. The penalty factor for two failed CEACs is sufficiently large that power must be maintained significantly < 100% RTP if CPC generated reactor trips are to be avoided. The Completion Time of 4 hours is adequate to accomplish these actions while minimizing risks.

The Required Actions are as follows:

B.1

Meeting the DNBR margin requirements of LCO 3.2.5, "AXIAL SHAPE INDEX (ASI)," ensures that power level and ASI are within a conservative region of operation based on actual core conditions. In addition to the above actions, the Reactor Power Cutback (RPCB) System must be disabled. This ensures that CEA position will not be affected by RPCB operation.

B.2

The "full out" CEA reed switches provide acceptable indication of CEA position. Therefore, the CEAs will remain fully withdrawn, except as required for specified testing or flux control via group #6. This verification ensures that undesired perturbations in local fuel burnup are prevented.

B.3

The "RSPT/CEAC Inoperable" addressable constant in each of the CPCs is set to indicate that both CEACs are inoperable. This provides a conservative penalty factor to ensure that a conservative effective margin is maintained by the CPCs in the computation of DNBR and LPD trips.

BASES

ACTIONS (continued)

B.4

The CEDMCS is placed and maintained in "OFF," except during CEA motion permitted by Required Action B.2, to prevent inadvertent motion and possible misalignment of the CEAs.

B.5

A comprehensive set of comparison checks on individual CEAs within groups must be made within 4 hours. Verification that each CEA is within 7 inches of other CEAs in its group provides a check that no CEA has deviated from its proper position within the group.

C.1

Condition C applies if the CPC channel B or C cabinet receives a high temperature alarm. There is one temperature sensor in each of the four CPC bays. Since CPC bays B and C also house CEAC calculators 1 and 2, respectively, a high temperature in either of these bays may also indicate a problem with the associated CEAC.

If a CPC channel B or C cabinet high temperature alarm is received, it is possible for the CEAC to be affected and not be completely reliable. Therefore, a CHANNEL FUNCTIONAL TEST must be performed within 12 hours. The Completion Time of 12 hours is adequate, considering the low probability of undetected failure, the consequences of failure, and the time required to perform a CHANNEL FUNCTIONAL TEST.

D.1

Condition D applies if an OPERABLE CEAC has three or more autorestarts in a 12 hour period.

CPCs and CEACs will attempt to autorestart if they detect a fault condition such as a calculator malfunction or loss of power. A successful autorestart restores the calculator to operation; however, excessive autorestarts might be indicative of a calculator problem.

BASES

ACTIONS (continued)

If a nonbypassed CEAC has three or more autorestarts, it may not be completely reliable. Therefore, a CHANNEL FUNCTIONAL TEST must be performed on the CEAC to ensure it is functioning properly. Based on plant operating experience, the Completion Time of 24 hours is adequate and reasonable to perform the test while still keeping the risk of operating in this condition at an acceptable level, since overt channel failure will most likely be indicated and annunciated by CPC online diagnostics.

E.1

Condition E is entered when the Required Action and associated Completion Time of Condition B, C, or D are not met.

If the Required Actions associated with these Conditions cannot be completed within the required Completion Time, the reactor must be brought to a MODE where the Required Actions do not apply. The Completion Time of 6 hours is reasonable, based on operating experience, for reaching the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

----------------------------------REVIEWER'S NOTE----------------------------------
In order for a plant to take credit for topical reports as the basis for justifying Frequencies, topical reports must be supported by an NRC staff Safety Evaluation Report that establishes the acceptability of each topical report for that plant (Ref. 4).

SR 3.3.3.1

Performance of the CHANNEL CHECK once every 12 hours ensures that gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the parameter indicated on one channel to a similar parameter on another channel. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value.

Significant deviations between the two instrument channels could be an indication of excessive instrument drift in one of the channels or of something even more serious. CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying that the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

BASES

SURVEILLANCE REQUIREMENTS (continued)

Agreement criteria are determined by the plant staff, based on a combination of the channel instrument uncertainties, including indication and readability. If a channel is outside the criteria, it may be an indication that the sensor or the signal processing equipment has drifted outside its limits.

The Frequency, about once every shift, is based on operating experience that demonstrates the rarity of channel failure. Since the probability of two random failures in redundant channels in any 12 hour period is extremely low, the CHANNEL CHECK minimizes the chance of loss of protective function due to failure of redundant channels. The CHANNEL CHECK supplements less formal, but more frequent, checks of channel OPERABILITY during normal operational use of the displays associated with the LCO required channels.

SR 3.3.3.2

The CEAC autorestart count is checked every 12 hours to monitor the CPC and CEAC for normal operation. If three or more autorestarts of a nonbypassed CPC occur within a 12 hour period, the CPC may not be completely reliable. Therefore, the Required Action of Condition D must be performed. The Frequency is based on operating experience that demonstrates the rarity of more than one channel failing within the same 12 hour interval.

SR 3.3.3.3

A CHANNEL FUNCTIONAL TEST on each CEAC channel is performed every 92 days to ensure the entire channel will perform its intended function when needed. The quarterly CHANNEL FUNCTIONAL TEST is performed using test software. The Frequency of 92 days is based on the reliability analysis presented in topical report CEN-327, "RPS/ESFAS Extended Test Interval Evaluation" (Ref. 5). A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.3.4

SR 3.3.3.4 is the performance of a CHANNEL CALIBRATION every [18] months.

CHANNEL CALIBRATION is a complete check of the instrument channel including the sensor. The Surveillance verifies that the channel responds to a measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drift between successive calibrations to ensure that the channel remains operational between successive surveillances. CHANNEL CALIBRATIONS must be performed consistent with the plant specific setpoint analysis.

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the surveillance interval extension analysis. The requirements for this review are outlined in Reference [5].

The Frequency is based upon the assumption of an [18] month calibration interval in the determination of the magnitude of equipment drift in the setpoint analysis and includes operating experience and consistency with the typical [18] month fuel cycle.

SR 3.3.3.5

Every [18] months, a CHANNEL FUNCTIONAL TEST is performed on the CEACs. The CHANNEL FUNCTIONAL TEST shall include the injection of a signal as close to the sensors as practicable to verify OPERABILITY, including alarm and trip Functions. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

The basis for the [18] month Frequency is that the CEACs perform a continuous self monitoring function that eliminates the need for frequent CHANNEL FUNCTIONAL TESTS. This CHANNEL FUNCTIONAL TEST essentially validates the self monitoring function and checks for a small set of failure modes that are undetectable by the self monitoring function. Operating experience has shown that undetected CPC or CEAC failures do not occur in any given [18] month interval.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.3.6

The isolation characteristics of each CEAC CEA position isolation amplifier and each optical isolator for CEAC to CPC data transfer are verified once per refueling to ensure that a fault in a CEAC or a CPC channel will not render another CEAC or CPC channel inoperable. The CEAC CEA position isolation amplifiers, mounted in CPC cabinets A and D, prevent a CEAC fault from propagating back to CPC A or D. The optical isolators for CPC to CEAC data transfer prevent a fault originating in any CPC channel from propagating back to any CEAC through this data link.

The Frequency is based on plant operating experience with regard to channel OPERABILITY, which demonstrates the failure of a channel in any [18] month interval is rare.

REFERENCES

1. 10 CFR 50.
2. 10 CFR 100.
3. FSAR, Section [7.2].
4. NRC Safety Evaluation Report, [Date].
5. CEN-327, June 2, 1986, including Supplement 1, March 3, 1989.

B 3.3 INSTRUMENTATION

B 3.3.4 Reactor Protective System (RPS) Logic and Trip Initiation (Digital)

BASES

BACKGROUND

The RPS initiates a reactor trip to protect against violating the core fuel design limits and reactor coolant pressure boundary integrity during anticipated operational occurrences (AOOs). By tripping the reactor, the RPS also assists the Engineered Safety Features (ESF) systems in mitigating accidents.

The protection and monitoring systems have been designed to ensure safe operation of the reactor. This is achieved by specifying limiting safety system settings (LSSS) in terms of parameters directly monitored by the RPS, as well as LCOs on other reactor system parameters and equipment performance.

The LSSS, defined in this Specification as the Allowable Value, in conjunction with the LCOs, establish the threshold for protective system action to prevent exceeding acceptable limits during Design Basis Accidents.

During AOOs, which are those events expected to occur one or more times during the plant life, the acceptable limits are:

- The departure from nucleate boiling ratio shall be maintained above the Safety Limit (SL) value to prevent departure from nucleate boiling,
- Fuel centerline melting shall not occur, and
- The Reactor Coolant System pressure SL of 2750 psia shall not be exceeded.

Maintaining the parameters within the above values ensures that the offsite dose will be within the 10 CFR 50 (Ref. 1) and 10 CFR 100 (Ref. 2) criteria during AOOs.

Accidents are events that are analyzed even though they are not expected to occur during the plant life. The acceptable limit during accidents is that the offsite dose shall be maintained within an acceptable fraction of 10 CFR 100 (Ref. 2) limits. Different accident categories allow a different fraction of these limits based on probability of occurrence. Meeting the acceptable dose limit for an accident category is considered having acceptable consequences for that event.

BASES

BACKGROUND (continued)

The RPS is segmented into four interconnected modules. These modules are:

- Measurement channels,
- Bistable trip units,
- RPS Logic, and
- Reactor trip circuit breakers (RTCBs).

This LCO addresses the RPS Logic and RTCBs, including Manual Trip capability. LCO 3.3.1, "Reactor Protective System (RPS) Instrumentation - Operating," provides a description of the role of this equipment in the RPS. This is summarized below:

<u>RPS Logic</u>

The RPS Logic, consisting of Matrix and Initiation Logic, employs a scheme that provides a reactor trip when bistables in any two of the four channels sense the same input parameter trip. This is called a two-out-of-four trip logic.

Bistable relay contact outputs from the four channels are configured into six logic matrices. Each logic matrix checks for a coincident trip in the same parameter in two bistable channels. The matrices are designated the AB, AC, AD, BC, BD, and CD matrices to reflect the bistable channels being monitored. Each logic matrix contains four normally energized matrix relays. When a coincidence is detected, consisting of a trip in the same Function in the two channels being monitored by the logic matrix, all four matrix relays de-energize.

The matrix relay contacts are arranged into trip paths, with one of the four matrix relays in each matrix opening contacts in one of the four trip paths. Each trip path provides power to one of the four normally energized RTCB control relays (K1, K2, K3, and K4). The trip paths thus each have six contacts in series, one from each matrix, and perform a logical <u>OR</u> function, opening the RTCBs if any one or more of the six logic matrices indicate a coincidence condition.

BASES

BACKGROUND (continued)

Each trip path is responsible for opening one set of two of the eight RTCBs. The RTCB control relays (K-relays), when de-energized, interrupt power to the breaker undervoltage trip attachments and simultaneously apply power to the shunt trip attachments on each of the two breakers. Actuation of either the undervoltage or shunt trip attachment is sufficient to open the RTCB and interrupt power from the motor generator (MG) sets to the control element drive mechanisms (CEDMs).

When a coincidence occurs in two RPS channels, all four matrix relays in the affected matrix de-energize. This in turn de-energizes all four breaker control relays, which simultaneously de-energize the undervoltage and energize the shunt trip attachments in all eight RTCBs, tripping them open.

Matrix Logic refers to the matrix power supplies, trip channel bypass contacts, and interconnecting matrix wiring between bistable relay cards, up to but not including the matrix relays. Matrix contacts on the bistable relay cards are excluded from the Matrix Logic definition, since they are addressed as part of the measurement channel.

The Initiation Logic consists of the trip path power source, matrix relays and their associated contacts, all interconnecting wiring, and solid state (auxiliary) relays through the K-relay contacts in the RTCB control circuitry.

It is possible to change the two-out-of-four RPS Logic to a two-out-of-three logic for a given input parameter in one channel at a time by trip channel bypassing select portions of the Matrix Logic. Trip channel bypassing a bistable effectively shorts the bistable relay contacts in the three matrices associated with that channel. Thus, the bistables will function normally, producing normal trip indication and annunciation, but a reactor trip will not occur unless two additional channels indicate a trip condition. Trip channel bypassing can be simultaneously performed on any number of parameters in any number of channels, providing each parameter is bypassed in only one channel at a time. An interlock prevents simultaneous trip channel bypassing of the same parameter in more than one channel. Trip channel bypassing is normally employed during maintenance or testing.

BASES

BACKGROUND (continued)

Reactor Trip Circuit Breakers (RTCBs)

The reactor trip switchgear consists of eight RTCBs, which are operated in four sets of two breakers (four channels). Power input to the reactor trip switchgear comes from two full capacity MG sets operated in parallel such that the loss of either MG set does not de-energize the CEDMs. There are two separate CEDM power supply buses, each bus powering half of the CEDMs. Power is supplied from the MG sets to each bus via two redundant paths (trip legs). Trip legs 1A and 1B supply power to CEDM bus 1. Trip legs 2A and 2B supply power to CEDM bus 2. This ensures that a fault or the opening of a breaker in one trip leg (i.e., for testing purposes) will not interrupt power to the CEDM buses.

Each of the four trip legs consists of two RTCBs in series. The two RTCBs within a trip leg are actuated by separate initiation circuits.

The eight RTCBs are operated as four sets of two breakers (four channels). For example, if a breaker receives an open signal in trip leg A (for CEDM bus 1), an identical breaker in trip leg B (for CEDM bus 2) will also receive an open signal. This arrangement ensures that power is interrupted to both CEDM buses, thus preventing trip of only half of the control element assemblies (CEAs) (a half trip). Any one inoperable breaker in a channel will make the entire channel inoperable.

Each set of RTCBs is operated by either a Manual Trip push button or an RPS actuated K-relay. There are four Manual Trip push buttons, arranged in two sets of two. Depressing both push buttons in either set will result in a reactor trip.

When a Manual Trip is initiated using the control room push buttons, the RPS trip paths and K-relays are bypassed, and the RTCB undervoltage and shunt trip attachments are actuated independent of the RPS.

Manual Trip circuitry includes the push button and interconnecting wiring to both RTCBs necessary to actuate both the undervoltage and shunt trip attachments, but excludes the K-relay contacts and their interconnecting wiring to the RTCBs, which are considered part of the Initiation Logic.

Functional testing of the entire RPS, from bistable input through the opening of the individual sets of RTCBs, can be performed either at power or shutdown and is normally performed on a quarterly basis. FSAR, Section [7.2] (Ref. 3), explains RPS testing in more detail.

BASES

APPLICABLE SAFETY ANALYSES

Reactor Protective System (RPS) Logic

The RPS Logic provides for automatic trip initiation to maintain the SLs during AOOs and assist the ESF systems in ensuring acceptable consequences during accidents. All transients and accidents that call for a reactor trip assume the RPS Logic is functioning as designed.

Reactor Trip Circuit Breakers (RTCBs)

All of the transient and accident analyses that call for a reactor trip assume that the RTCBs operate and interrupt power to the CEDMs.

Manual Trip

There are no accident analyses that take credit for the Manual Trip; however, the Manual Trip is part of the RPS circuitry. It is used by the operator to shut down the reactor whenever any parameter is rapidly trending toward its trip setpoint. A Manual Trip accomplishes the same results as any one of the automatic trip Functions.

The RPS instrumentation satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

Reactor Protective System (RPS) Logic

The LCO on the RPS Logic channels ensures that each of the following requirements are met:

- A reactor trip will be initiated when necessary,
- The required protection system coincidence logic is maintained (minimum two-out-of-three, normal two-out-of-four), and
- Sufficient redundancy is maintained to permit a channel to be out of service for testing or maintenance.

Failures of individual bistable relays and their contacts are addressed in LCO 3.3.1. This Specification addresses failures of the Matrix Logic not addressed in the above, such as the failure of matrix relay power supplies or the failure of the trip channel bypass contact in the bypass condition.

BASES

LCO (continued)

Loss of a single vital bus will de-energize one of the two power supplies in each of three matrices. This will result in four RTCBs opening; however, the remaining four closed RTCBs will prevent a reactor trip. For the purposes of this LCO, de-energizing up to three matrix power supplies due to a single failure is to be treated as a single channel failure, providing the affected matrix relays de-energize as designed, opening the affected RTCBs.

Each of the four Initiation Logic channels opens one set of RTCBs if any of the six coincidence matrices de-energize their associated matrix relays. They thus perform a logical <u>OR</u> function. Each Initiation Logic channel has its own power supply and is independent of the others. An Initiation Logic channel includes the matrix relay through to the K-relay contacts, which open the RTCB.

It is possible for two Initiation Logic channels affecting the same trip leg to de-energize if a matrix power supply or vital instrument bus fails. This will result in opening the two affected sets of RTCBs.

If one set of RTCBs has been opened in response to a single RTCB channel, Initiation Logic channel, or Manual Trip channel failure, the affected set of RTCBs may be closed for up to 1 hour for Surveillance on the OPERABLE Initiation Logic, RTCB, and Manual Trip channels. In this case, the redundant set of RTCBs will provide protection if a trip should be required. It is unlikely that a trip will be required during the Surveillance, coincident with a failure of the remaining series RTCB channel. If a single matrix power supply or vital bus failure has opened two sets of RTCBs, Manual Trip and RTCB testing on the closed breakers cannot be performed without causing a trip.

1. <u>Matrix Logic</u>

   This LCO requires six channels of Matrix Logic to be OPERABLE in MODES 1 and 2, and in MODES 3, 4, and 5 when any RTCBs are closed and any CEA is capable of being withdrawn.

2. <u>Initiation Logic</u>

   This LCO requires four channels of Initiation Logic to be OPERABLE in MODES 1 and 2, and in MODES 3, 4, and 5 when the RTCBs are closed and any CEA is capable of being withdrawn.

BASES

LCO (continued)

3. Reactor Trip Circuit Breakers

The LCO requires four RTCB channels to be OPERABLE in MODES 1 and 2, as well as in MODES 3, 4, and 5 when the RTCBs are closed and any CEA is capable of being withdrawn.

Each channel consists of two breakers operated in a single set by the Initiation Logic or Manual Trip circuitry. This ensures that power is interrupted at identical locations in the trip legs for both CEDM buses, thus preventing power removal to only one CEDM bus (a half trip).

Failure of a single breaker affects the entire channel, and both breakers in the set must be opened. Without reliable RTCBs and associated support circuitry, a reactor trip cannot occur whether initiated automatically or manually.

Each channel of RTCBs starts at the contacts that are actuated by the K-relay and the Manual Trip for each set of breakers. The K-relay actuated contacts and the upstream circuitry are considered to be RPS Logic. Manual Trip contacts and upstream circuitry are considered to be Manual Trip circuitry.

A Note associated with the ACTIONS states that if one set of RTCBs has been opened in response to a single RTCB channel, Initiation Logic channel, or Manual Trip channel failure, the affected set of RTCBs may be closed for up to 1 hour for Surveillance on the OPERABLE Initiation Logic, RTCB, and Manual Trip channels. In this case the redundant set of RTCBs will provide protection. If a single matrix power supply or vital bus failure has opened two sets of RTCBs, Manual Trip and RTCB testing on the closed breakers cannot be performed without causing a trip.

4. Manual Trip

The LCO requires all four Manual Trip channels to be OPERABLE in MODES 1 and 2, and MODES 3, 4, and 5 when the RTCBs are closed and any CEA is capable of being withdrawn.

Two independent sets of two adjacent push buttons are provided at separate locations. Each push button is considered a channel and operates two of the eight RTCBs. Depressing both push buttons in either channel will cause an interruption of power to the CEDMs, allowing the CEAs to fall into the core. This design ensures that no single failure in any push button circuit can either cause or prevent a reactor trip.

BASES

LCO (continued)

Manual Trip push buttons are also provided at the reactor trip switchgear (locally) in case the control room push buttons become inoperable or the control room becomes uninhabitable. These are not part of the RPS and cannot be credited in fulfilling the LCO OPERABILITY requirements. Furthermore, LCO ACTIONS need not be entered due to failure of a local Manual Trip.

APPLICABILITY

The RPS Logic, RTCBs, and Manual Trip are required to be OPERABLE in any MODE when the CEAs are capable of being withdrawn off the bottom of the core (i.e., RTCBs closed and power available to the CEDMs). This ensures that the reactor can be tripped when necessary, but allows for maintenance and testing when the reactor trip is not needed.

In MODES 3, 4, and 5 with the RTCBs open, the CEAs are not capable of withdrawal and these Functions do not have to be OPERABLE. However, two logarithmic power level channels must be OPERABLE to ensure proper indication of neutron population and to indicate a boron dilution event. This is addressed in LCO 3.3.13, "[Logarithmic] Power Monitoring Channels."

ACTIONS

When the number of inoperable channels in a trip Function exceeds that specified in any related Condition associated with the same trip Function, then the plant is outside the safety analysis. Therefore, LCO 3.0.3 is immediately entered if applicable in the current MODE of operation.

<u>A.1</u>

Condition A applies if one Matrix Logic channel is inoperable or three Matrix Logic channels are inoperable due to a common power source failure de-energizing three matrix power supplies in any applicable MODE. Loss of a single vital instrument bus will de-energize one of the two matrix power supplies in up to three matrices. This is considered a single matrix failure, providing the matrix relays associated with the failed power supplies de-energize as required.

The channel must be restored to OPERABLE status within 48 hours. The Completion Time of 48 hours provides the operator time to take appropriate actions and still ensures that any risk involved in operating with a failed channel is acceptable. Operating experience has demonstrated that the probability of a random failure of a second Matrix Logic channel is low during any given 48 hour interval. If the channel cannot be restored to OPERABLE status within 48 hours, Condition E is entered.

BASES

ACTIONS (continued)

B.1

Condition B applies to one Initiation Logic channel, RTCB channel, or Manual Trip channel in MODES 1 and 2, since they have the same actions. MODES 3, 4, and 5, with the RTCBs shut, are addressed in Condition C. These Required Actions require opening the affected RTCBs. This removes the need for the affected channel by performing its associated safety function. With an RTCB open, the affected Functions are in one-out-of-two logic, which meets redundancy requirements, but testing on the OPERABLE channels cannot be performed without causing a reactor trip unless the RTCBs in the inoperable channels are closed to permit testing.

Required Action B.1 provides for opening the RTCBs associated with the inoperable channel within a Completion Time of 1 hour. This Required Action is conservative, since depressing the Manual Trip push button associated with either set of breakers in the other trip leg will cause a reactor trip. With this configuration, a single channel failure will not prevent a reactor trip. The allotted Completion Time is adequate for opening the affected RTCBs while maintaining the risk of having them closed at an acceptable level.

C.1

Condition C applies to the failure of one Initiation Logic channel, RTCB channel, or Manual Trip channel affecting the same trip leg in MODE 3, 4, or 5 with the RTCBs closed. The channel must be restored to OPERABLE status within 48 hours. If the inoperable channel cannot be restored to OPERABLE status within 48 hours, the affected RTCBs must be opened. In some cases, this condition may effect all of the RTCBs. This removes the need for the affected channel by performing its associated safety function. With the RTCBs open, the affected functions are in a one-out-of-two logic, which meets redundancy requirements.

The Completion Time of 48 hours is consistent with that of other RPS instrumentation and should be adequate to repair most failures.

Testing on the OPERABLE channels cannot be performed without causing a reactor trip unless the RTCBs in the inoperable channels are closed to permit testing.

BASES

ACTIONS (continued)

D.1

Condition D applies to the failure of both Manual Trip or Initiation Logic channels affecting the same trip leg. Since this will open two channels of RTCBs, this Condition is also applicable to channels in the same trip leg. This will open both sets of RTCBs in the affected trip leg, satisfying the Required Action of opening the affected RTCBs.

Of greater concern is the failure of the initiation circuit in a nontrip condition (e.g., due to two initiation K-relay failures). With only one Initiation Logic channel failed in a nontrip condition, there is still the redundant set of RTCBs in the trip leg. With both failed in a nontrip condition, the reactor will not trip automatically when required. In either case, the affected RTCBs must be opened immediately by using the appropriate Manual Trip push buttons, since each of the four push buttons opens one set of RTCBs, independent of the initiation circuitry. Caution must be exercised, since depressing the wrong push buttons may result in a reactor trip.

If two Manual Trip channels are inoperable and affecting the same trip leg, the associated RTCBs must be opened immediately to ensure Manual Trip capability is maintained. With the affected RTCBs open, any one of two Manual Trip push buttons being depressed will result in a reactor trip.

If the affected RTCB cannot be opened, Required Action E is entered. This would only occur if there is a failure in the Manual Trip circuitry or the RTCB(s).

E.1 and E.2

Condition E is entered if Required Actions associated with Condition A, B, or D are not met within the required Completion Time or, if for one or more Functions, more than one Manual Trip, Matrix Logic, Initiation Logic, or RTCB channel is inoperable for reasons other than Condition A or D.

If the RTCBs associated with the inoperable channel cannot be opened, the reactor must be shut down within 6 hours and all the RTCBs opened. A Completion Time of 6 hours is reasonable, based on operating experience, for reaching the required plant conditions from full power conditions in an orderly manner and without challenging plant systems and for opening RTCBs. All RTCBs should then be opened, placing the plant in a MODE where the LCO does not apply and ensuring no CEA withdrawal occurs.

BASES

SURVEILLANCE REQUIREMENTS

-----------------------------------REVIEWER'S NOTE-----------------------------------
In order for a unit to take credit for topical reports as the basis for justifying Frequencies, topical reports must be supported by an NRC staff Safety Evaluation Report that establishes the acceptability of each topical report for that unit (Ref. 4).

SR 3.3.4.1

A CHANNEL FUNCTIONAL TEST is performed on each RTCB channel every 31 days. This verifies proper operation of each RTCB. The RTCB must then be closed prior to testing the other RTCBs, or a reactor trip may result. The Frequency of 31 days is based on the reliability analysis presented in Topical Report CEN-327, "RPS/ESFAS Extended Test Interval Evaluation," (Ref. 4).

SR 3.3.4.2

A CHANNEL FUNCTIONAL TEST on each RPS Logic channel is performed every [92] days to ensure the entire channel will perform its intended function when needed. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

In addition to power supply tests, the RPS CHANNEL FUNCTIONAL TEST consists of three overlapping tests as described in Reference 3. These tests verify that the RPS is capable of performing its intended function, from bistable input through the RTCBs. The first test, the bistable test, is addressed by SR 3.3.1.7 in LCO 3.3.1.

This SR addresses the two tests associated with the RPS Logic: Matrix Logic and Trip Path.

BASES

SURVEILLANCE REQUIREMENTS (continued)

Matrix Logic Tests

These tests are performed one matrix at a time. They verify that a coincidence in the two input channels for each Function removes power from the matrix relays. During testing, power is applied to the matrix relay test coils and prevents the matrix relay contacts from assuming their de-energized state. The Matrix Logic tests will detect any short circuits around the bistable contacts in the coincidence logic such as may be caused by faulty bistable relay or trip channel bypass contacts.

Trip Path Tests

These tests are similar to the Matrix Logic tests, except that test power is withheld from one matrix relay at a time, allowing the initiation circuit to de-energize, opening the affected set of RTCBs. The RTCBs must then be closed prior to testing the other three initiation circuits, or a reactor trip may result.

The Frequency of [92] days is based on the reliability analysis presented in topical report CEN-327, "RPS/ESFAS Extended Test Interval Evaluation" (Ref. 5).

Additionally, operating experience has shown that these components usually pass the Surveillance when performed at a Frequency of once every 7 days prior to each reactor startup.

SR 3.3.4.3

Each RTCB is actuated by an undervoltage coil and a shunt trip coil. The system is designed so that either de-energizing the undervoltage coil or energizing the shunt trip coil will cause the circuit breaker to open. When an RTCB is opened, either during an automatic reactor trip or by using the manual push buttons in the control room, the undervoltage coil is de-energized and the shunt trip coil is energized. This makes it impossible to determine if one of the coils or associated circuitry is defective.

BASES

SURVEILLANCE REQUIREMENTS (continued)

Therefore, once every [18] months, a CHANNEL FUNCTIONAL TEST is performed that individually tests all four sets of undervoltage coils and all four sets of shunt trip coils. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions. During undervoltage coil testing, the shunt trip coils must remain de-energized, preventing their operation. Conversely, during shunt trip coil testing, the undervoltage coils must remain energized, preventing their operation. This Surveillance ensures that every undervoltage coil and every shunt trip coil is capable of performing its intended function and that no single active failure of any RTCB component will prevent a reactor trip. The 18 month Frequency is based on the need to perform this Surveillance under the conditions that apply during a plant outage and the potential for an unplanned transient if the Surveillance were performed with the reactor at power. Operating experience has shown these components usually pass the Surveillance when performed at the Frequency of once every [18] months.

<u>SR 3.3.4.4</u>

A CHANNEL FUNCTIONAL TEST on the Manual Trip channels is performed prior to a reactor startup to ensure the entire channel will perform its intended function if required. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions. The Manual Trip Function can only be tested at shutdown. However, the simplicity of this circuitry and the absence of drift concern make this Frequency adequate.

REFERENCES

1. 10 CFR 50, Appendix A.

2. 10 CFR 100.

3. FSAR, Section [7.2].

4. CEN-327, June 2, 1986, including Supplement 1, March 3, 1989.

B 3.3 INSTRUMENTATION

B 3.3.5 Engineered Safety Features Actuation System (ESFAS) Instrumentation (Digital)

BASES

BACKGROUND

The ESFAS initiates necessary safety systems, based upon the values of selected unit parameters, to protect against violating core design limits and the Reactor Coolant System (RCS) pressure boundary during anticipated operational occurrences (AOOs) and ensures acceptable consequences during accidents.

The ESFAS contains devices and circuitry that generate the following signals when monitored variables reach levels that are indicative of conditions requiring protective action:

1. Safety Injection Actuation Signal (SIAS), Containment Cooling Actuation Signal (CCAS) (actuated by an automatic SIAS),
2. Containment Spray Actuation Signal (CSAS),
3. Containment Isolation Actuation Signal (CIAS),
4. Main Steam Isolation Signal (MSIS),
5. Recirculation Actuation Signal (RAS), and

6, 7. Emergency Feedwater Actuation Signal (EFAS).

Equipment actuated by each of the above signals is identified in the FSAR (Ref. 1).

Each of the above ESFAS instrumentation systems is segmented into three interconnected modules. These modules are:

- Measurement channels,
- Bistable trip units, and
- ESFAS Logic:
  - Matrix Logic,
  - Initiation Logic (trip paths), and
  - Actuation Logic.

BASES

BACKGROUND (continued)

This LCO addresses measurement channels and bistables. Logic is addressed in LCO 3.3.6, "Engineered Safety Features Actuation System (ESFAS) Logic and Manual Trip."

The role of each of these modules in the ESFAS, including the logic of LCO 3.3.6, is discussed below.

Measurement Channels

Measurement channels, consisting of field transmitters or process sensors and associated instrumentation, provide a measurable electronic signal based upon the physical characteristics of the parameter being measured.

Four identical measurement channels with electrical and physical separation are provided for each parameter used in the generation of trip signals. These channels are designated A through D. Measurement channels provide input to ESFAS bistables within the same ESFAS channel. In addition, some measurement channels are used as inputs to Reactor Protective System (RPS) bistables, and most provide indication in the control room. Measurement channels used as an input to the RPS or ESFAS are not used for control Functions.

When a channel monitoring a parameter indicates an unsafe condition, the bistable monitoring the parameter in that channel will trip. Tripping two or more channels of bistables monitoring the same parameter will de-energize Matrix Logic, which in turn de-energizes the Initiation Logic. This causes both channels of Actuation Logic to de-energize. Each channel of Actuation Logic controls one train of the associated Engineered Safety Features (ESF) equipment.

Three of the four measurement and bistable channels are necessary to meet the redundancy and testability of GDC 21 in Appendix A to 10 CFR 50 (Ref. 2). The fourth channel provides additional flexibility by allowing one channel to be removed from service (trip channel bypass) for maintenance or testing while still maintaining a minimum two-out-of-three logic.

BASES

BACKGROUND (continued)

-----------------------------------REVIEWER'S NOTE-----------------------------------
In order to take full advantage of the four channel design, adequate channel to channel independence must be demonstrated and approved by the NRC staff. Plants not currently licensed to credit four channel independence that may desire this capability must have approval of the NRC staff, documented by an NRC Safety Evaluation Report (Ref. 3). Adequate channel to channel independence includes physical and electrical independence of each channel from the others. Furthermore, each channel must be energized from separate inverters and station batteries. Plants that have demonstrated adequate channel to channel independence may operate in two-out-of-three logic configuration, with one channel removed from service, until following the next MODE 5 entry. Plants not demonstrating four channel independence can only operate for 48 hours with one channel inoperable (Ref. 3).

Since no single failure will either cause or prevent a protective system actuation, and no protective channel feeds a control channel, this arrangement meets the requirements of IEEE Standard 279-1971 (Ref. 4).

Bistable Trip Units

Bistable trip units, mounted in the Plant Protection System (PPS) cabinet, receive an analog input from the measurement channels, compare the analog input to trip setpoints, and provide contact output to the Matrix Logic for each ESFAS Function. They also provide local trip indication and remote annunciation.

There are four channels of bistables, designated A through D, for each ESFAS Function, one for each measurement channel. In cases where two ESF Functions share the same input and trip setpoint (e.g., containment pressure input to CIAS and SIAS), the same bistable may be used to satisfy both Functions. Similarly, bistables may be shared between the RPS and ESFAS (e.g., Pressurizer Pressure - Low input to the RPS and SIAS). Bistable output relays de-energize when a trip occurs, in turn de-energizing bistable relays mounted in the PPS relay card racks.

The contacts from these bistable relays are arranged into six coincidence matrices, comprising the Matrix Logic. If bistables monitoring the same parameter in at least two channels trip, the Matrix Logic will generate an ESF actuation (two-out-of-four logic).

BASES

BACKGROUND (continued)

The trip setpoints and Allowable Values used in the bistables are based on the analytical limits stated in Reference 5. The selection of these trip setpoints is such that adequate protection is provided when all sensor and processing time delays are taken into account. To allow for calibration tolerances, instrumentation uncertainties, instrument drift, and severe environment effects, for those ESFAS channels that must function in harsh environments as defined by 10 CFR 50.49 (Ref. 6), Allowable Values specified in Table 3.3.5-1, in the accompanying LCO, are conservatively adjusted with respect to the analytical limits. A detailed description of the methodology used to calculate the trip setpoints, including their explicit uncertainties, is provided in the "Plant Protection System Selection of Trip Setpoint Values" (Ref. 7). The actual nominal trip setpoint entered into the bistable is normally still more conservative than that specified by the Allowable Value to account for changes in random measurement errors detectable by a CHANNEL FUNCTIONAL TEST. A channel is inoperable if its actual trip setpoint is not within its required Allowable Value.

Setpoints in accordance with the Allowable Value will ensure that Safety Limits of LCO Section 2.0, "Safety Limits," are not violated during AOOs and the consequences of Design Basis Accidents (DBAs) will be acceptable, providing the plant is operated from within the LCOs at the onset of the AOO or DBA and the equipment functions as designed.

Functional testing of the ESFAS, from the bistable input through the opening of initiation relay contacts in the ESFAS Actuation Logic, can be performed either at power or at shutdown and is normally performed on a quarterly basis. FSAR, Section [7.2] (Ref. 8), provides more detail on ESFAS testing. Process transmitter calibration is normally performed on a refueling basis. SRs for the channels are specified in the Surveillance Requirements section.

<u>ESFAS Logic</u>

The ESFAS Logic, consisting of Matrix, Initiation and Actuation Logic, employs a scheme that provides an ESF actuation of both trains when bistables in any two of the four channels sense the same input parameter trip. This is called a two-out-of-four trip logic.

BASES

BACKGROUND (continued)

Bistable relay contact outputs from the four channels are configured into six logic matrices. Each logic matrix checks for a coincident trip in the same parameter in two bistable channels. The matrices are designated the AB, AC, AD, BC, BD, and CD matrices to reflect the bistable channels being monitored. Each logic matrix contains four normally energized matrix relays. When a coincidence is detected in the two channels being monitored by the logic matrix, all four matrix relays de-energize.

The matrix relay contacts are arranged into trip paths, with one relay contact from each matrix relay in each of the four trip paths. Each trip path controls two initiation relays. Each of the two initiation relays in each trip path controls contacts in the Actuation Logic for one train of ESF.

Each of the two channels of Actuation Logic, mounted in the Auxiliary Relay Cabinet (ARCs), is responsible for actuating one train of ESF equipment. Each ESF Function has separate Actuation Logic in each ARC.

The contacts from the Initiation Logic are configured in a selective two-out-of-four logic in the Actuation Logic, similar to the configuration employed by the RPS in the RTCBs. This logic controls ARC mounted subgroup relays, which are normally energized. Contacts from these relays, when de-energized, actuate specific ESF equipment.

When a coincidence occurs in two ESFAS channels, all four matrix relays in the affected matrix will de-energize. This in turn will de-energize all eight initiation relays, four used in each Actuation Logic.

Matrix Logic refers to the matrix power supplies, trip channel bypass contacts, and interconnecting matrix wiring between bistable relay cards, up to but not including the matrix relays. Matrix contacts on the bistable relay cards are excluded from the Matrix Logic definition, since they are addressed as part of the measurement channel.

Initiation Logic consists of the trip path power source, matrix relays and their associated contacts, all interconnecting wiring, and the initiation relays.

Actuation Logic consists of all circuitry housed within the ARCs used to actuate the ESF Function, excluding the subgroup relays, and interconnecting wiring to the initiation relay contacts mounted in the PPS cabinet.

BASES

BACKGROUND (continued)

The subgroup relays are actuated by the ESFAS logic. Each ESFAS Function typically employs several subgroup relays, with each subgroup relay responsible for actuating one or more components in the ESFAS Function. Subgroup relays and their contacts are considered part of the actuated equipment and are addressed under the applicable LCO for this equipment. Initiation and Actuation Logic up to the subgroup relays is addressed in LCO 3.3.6.

It is possible to change the two-out-of-four ESFAS logic to a two-out-of-three logic for a given input parameter in one channel at a time by trip channel bypassing select portions of the Matrix Logic. Trip channel bypassing a bistable effectively shorts the bistable relay contacts in the three matrices associated with that channel. Thus, the bistables will function normally, producing normal trip indication and annunciation, but ESFAS actuation will not occur since the bypassed channel is effectively removed from the coincidence logic. Trip channel bypassing can be simultaneously performed on any number of parameters in any number of channels, providing each parameter is bypassed in only one channel at a time. An interlock prevents simultaneous trip channel bypassing of the same parameter in more than one channel. Trip channel bypassing is normally employed during maintenance or testing.

----------------------------------REVIEWER'S NOTE----------------------------------
For plants that have demonstrated sufficient channel to channel independence, two-out-of-three logic is the minimum that is required to provide adequate plant protection, since a failure of one channel still ensures ESFAS actuation would be generated by the two remaining OPERABLE channels. Two-out-of-three logic also prevents inadvertent actuations caused by any single channel failure in a trip condition.

In addition to the trip channel bypasses, there are also operating bypasses on select ESFAS actuation trips. These bypasses are enabled manually in all four channels when plant conditions do not warrant the specific trip protection. All operating bypasses are automatically removed when enabling bypass conditions are no longer satisfied. Operating bypasses normally are implemented in the bistable, so that normal trip indication is also disabled. The Pressurizer Pressure - Low input to the SIAS shares an operating bypass with the Pressurizer Pressure - Low reactor trip.

BASES

BACKGROUND (continued)

Manual ESFAS initiation capability is provided to permit the operator to manually actuate an ESF System when necessary.

Two sets of two push buttons (located in the control room) for each ESF Function are provided, and each set actuates both trains. Each Manual Trip push button opens one trip path, de-energizing one set of two initiation relays, one affecting each train of ESF. Initiation relay contacts are arranged in a selective two-out-of-four configuration in the Actuation Logic. By arranging the push buttons in two sets of two, such that both push buttons in a set must be depressed, it is possible to ensure that Manual Trip will not be prevented in the event of a single random failure. Each set of two push buttons is designated a single channel in LCO 3.3.6.

APPLICABLE SAFETY ANALYSES

Each of the analyzed accidents can be detected by one or more ESFAS Functions. One of the ESFAS Functions is the primary actuation signal for that accident. An ESFAS Function may be the primary actuation signal for more than one type of accident. An ESFAS Function may also be the secondary, or backup, actuation signal for one or more other accidents.

ESFAS protective Functions are as follows:

1. <u>Safety Injection Actuation Signal</u>

   SIAS ensures acceptable consequences during large break loss of coolant accidents (LOCAs), small break LOCAs, control element assembly ejection accidents, and main steam line breaks (MSLBs) inside containment. To provide the required protection, either a high containment pressure or a low pressurizer pressure signal will initiate SIAS. SIAS initiates the Emergency Core Cooling Systems (ECCS) and performs several other functions such as initiating a containment cooling actuation, initiating control room isolation, and starting the diesel generators.

   CCAS mitigates containment overpressurization when required by either a manual CCAS actuation or an automatic SIAS Function. This Function is not employed by all plants.

BASES

APPLICABLE SAFETY ANALYSES (continued)

2. Containment Spray Actuation Signal

CSAS actuates containment spray, preventing containment overpressurization during large break LOCAs, small break LOCAs, and MSLBs or feedwater line breaks (FWLBs) inside containment. CSAS is initiated by high containment pressure and an SIAS. This configuration reduces the likelihood of inadvertent containment spray.

3. Containment Isolation Actuation Signal

CIAS ensures acceptable mitigating actions during large and small break LOCAs, and MSLBs or FWLBs either inside or outside containment. CIAS is initiated by low pressurizer pressure or high containment pressure.

4. Main Steam Isolation Signal

MSIS ensures acceptable consequences during an MSLB or FWLB (between the steam generator and the main feedwater check valve), either inside or outside containment. MSIS isolates both steam generators if either generator indicates a low pressure condition or if a high containment pressure condition exists. This prevents an excessive rate of heat extraction and subsequent cooldown of the RCS during these events.

5. Recirculation Actuation Signal

At the end of the injection phase of a LOCA, the refueling water storage tank (RWST) will be nearly empty. Continued cooling must be provided by the ECCS to remove decay heat. The source of water for the ECCS pumps is automatically switched to the containment recirculation sump. Switchover from RWST to containment sump must occur before the RWST empties to prevent damage to the ECCS pumps and a loss of core cooling capability. For similar reasons, switchover must not occur before there is sufficient water in the containment sump to support pump suction. Furthermore, early switchover must not occur to ensure sufficient borated water is injected from the RWST to ensure the reactor remains shut down in the recirculation mode. An RWST Level - Low signal initiates the RAS.

BASES

APPLICABLE SAFETY ANALYSES (continued)

6, 7. Emergency Feedwater Actuation Signal

EFAS consists of two steam generator (SG) specific signals (EFAS-1 and EFAS-2). EFAS-1 initiates emergency feed to SG #1, and EFAS-2 initiates emergency feed to SG #2.

EFAS maintains a steam generator heat sink during a steam generator tube rupture event and an MSLB or FWLB event either inside or outside containment.

Low steam generator water level initiates emergency feed to the affected steam generator, providing the generator is not identified (by the circuitry) as faulted (a steam or FWLB).

EFAS logic includes steam generator specific inputs from the Steam Generator Pressure - Low bistable comparator (also used in MSIS) and the SG Pressure Difference - High (SG #1 > SG #2 or SG #2 > SG #1, bistable comparators) to determine if a rupture in either generator has occurred.

Rupture is assumed if the affected generator has a low pressure condition, unless that generator is significantly higher in pressure than the other generator.

This latter feature allows feeding the intact steam generator, even if both are below the MSIS setpoint, while preventing the ruptured generator from being fed. Not feeding a ruptured generator prevents containment overpressurization during the analyzed events.

The ESFAS satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

The LCO requires all channel components necessary to provide an ESFAS actuation to be OPERABLE.

Plants are restricted to 48 hours in a trip channel bypass condition before restoring the Function to four channel operation (two-out-of-four logic) or placing the channel in trip (two-out-of-three logic).

The Bases for the LCOs on ESFAS Functions are:

BASES

LCO (continued)

1. Safety Injection Actuation Signal

   a. Containment Pressure - High

      This LCO requires four channels of Containment Pressure - High to be OPERABLE in MODES 1, 2, and 3.

      The Containment Pressure - High signal is shared among the SIAS (Function 1), CIAS (Function 3), and MSIS (Function 4).

      The Allowable Value for this trip is set high enough to allow for small pressure increases in containment expected during normal operation (i.e., plant heatup) and is not indicative of an abnormal condition. The setting is low enough to initiate the ESF Functions when an abnormal condition is indicated. This allows the ESF systems to perform as expected in the accident analyses to mitigate the consequences of the analyzed accidents.

   b. Pressurizer Pressure - Low

      This LCO requires four channels of Pressurizer Pressure - Low to be OPERABLE in MODES 1 and 2.

      The Allowable Value for this trip is set low enough to prevent actuating the ESF Functions (SIAS and CIAS) during normal plant operation and pressurizer pressure transients. The setting is high enough that, with the specified accidents, the ESF systems will actuate to perform as expected, mitigating the consequences of the accident.

      The Pressurizer Pressure - Low trip setpoint, which provides SIAS, CIAS, and RPS trip, may be manually decreased to a floor value of 300 psia to allow for a controlled cooldown and depressurization of the RCS without causing a reactor trip, CIAS, or SIAS. The margin between actual pressurizer pressure and the trip setpoint must be maintained less than or equal to the specified value (400 psia) to ensure a reactor trip, CIAS, and SIAS will occur if required during RCS cooldown and depressurization.

      From this reduced setting, the trip setpoint will increase automatically as pressurizer pressure increases, tracking actual RCS pressure until the trip setpoint is reached.

BASES

LCO (continued)

When the trip setpoint has been lowered below the bypass permissive setpoint of 400 psia, the Pressurizer Pressure - Low reactor trip, CIAS, and SIAS actuation may be manually bypassed in preparation for shutdown cooling. When RCS pressure rises above the bypass removal setpoint, the bypass is removed.

Bypass Removal

This LCO requires four channels of bypass removal for Pressurizer Pressure - Low to be OPERABLE in MODES 1, 2, and 3.

Each of the four channels enables and disables the bypass capability for a single channel. Therefore, this LCO applies to the bypass removal feature only. If the bypass enable function is failed so as to prevent entering a bypass condition, operation may continue. Because the trip setpoint has a floor value of 300 psia, a channel trip will result if pressure is decreased below this setpoint without bypassing.

The bypass removal Allowable Value was chosen because MSLB events originating from below this setpoint add less positive reactivity than that which can be compensated for by required SDM.

2. Containment Spray Actuation Signal

CSAS is initiated either manually or automatically. For an automatic actuation, it is necessary to have a Containment Pressure - High High signal, coincident with an SIAS. The SIAS requirement should always be satisfied on a legitimate CSAS, since the Containment Pressure - High signal used in the SIAS will initiate before the Containment Pressure - High High. This ensures that a CSAS will not initiate unless required.

a. Containment Pressure - High High

This LCO requires four channels of Containment Pressure - High High to be OPERABLE in MODES 1, 2, and 3.

BASES

LCO (continued)

The Allowable Value for this trip is set high enough to allow for first response ESF systems (containment cooling systems) to attempt to mitigate the consequences of an accident before resorting to spraying borated water onto containment equipment. The setting is low enough to initiate CSAS in time to prevent containment pressure from exceeding design.

3. Containment Isolation Actuation Signal

For plants where the SIAS and CIAS are actuated on Pressurizer Pressure - Low or Containment Pressure - High, the SIAS and CIAS share the same input channels, bistables, and matrices and matrix relays. The remainder of the initiation channels, the manual channels, and the Actuation Logic are separate and are addressed in LCO 3.3.6. Since their Applicability is also the same, they have identical Required Actions.

a. Containment Pressure - High

This LCO requires four channels of Containment Pressure - High to be OPERABLE in MODES 1, 2, and 3.

The Containment Pressure - High signal is shared among the SIAS (Function 1), CIAS (Function 3), and MSIS (Function 4).

The Allowable Value for this trip is set high enough to allow for small pressure increases in containment expected during normal operation (i.e., plant heatup) and is not indicative of an abnormal condition. The setting is low enough to initiate the ESF Functions when an abnormal condition is indicated. This allows the ESF systems to perform as expected in the accident analyses to mitigate the consequences of the analyzed accidents.

b. Pressurizer Pressure - Low

This LCO requires four channels of Pressurizer Pressure - Low to be OPERABLE in MODES 1, 2, and 3.

The Allowable Value for this trip is set low enough to prevent actuating the ESF Functions (SIAS and CIAS) during normal plant operation and pressurizer pressure transients. The setting is high enough that, with the specified accident, the ESF systems will actuate to perform as expected, mitigating the consequences of the accidents.

BASES

LCO (continued)

The Pressurizer Pressure - Low trip setpoint, which provides an SIAS, CIAS, and RPS trip, may be manually decreased to a floor Allowable Value of 300 psia to allow for a controlled cooldown and depressurization of the RCS without causing a reactor trip, CIAS or SIAS. The safety margin between actual pressurizer pressure and the trip setpoint must be maintained less than or equal to the specified value (400 psi) to ensure a reactor trip, CIAS, and SIAS will occur if required during RCS cooldown and depressurization.

From this reduced setting, the trip setpoint will increase automatically as pressurizer pressure increases, tracking actual RCS pressure until the trip setpoint is reached.

When the trip setpoint has been lowered below the bypass removal setpoint of 400 psia, the Pressurizer Pressure - Low reactor trip, CIAS, and SIAS actuation may be manually bypassed in preparation for shutdown cooling. When RCS pressure rises above the bypass removal, the bypass is removed.

Bypass Removal

This LCO requires four channels of bypass removal for Pressurizer Pressure - Low to be OPERABLE in MODES 1, 2, and 3.

Each of the four channels enables and disables the bypass capability for a single channel. Therefore all four bypass removal channels must be OPERABLE to ensure that none of the four channels are inadvertently bypassed.

This LCO applies to the bypass removal feature only. If the bypass enable function is failed so as to prevent entering a bypass condition, operation may continue. Because the trip setpoint has a floor value of 300 psia, a channel trip will result if pressure is decreased below this setpoint without bypassing.

The bypass removal Allowable Value was chosen because MSLB events originating from below this setpoint add less positive reactivity than that which can be compensated for by required SDM.

BASES

LCO (continued)

4. Main Steam Isolation Signal

The LCO is applicable to the MSIS in MODES 1, 2, and 3 except when all associated valves are closed and de-activated.

a. Steam Generator Pressure - Low

This LCO requires four channels of Steam Generator Pressure - Low to be OPERABLE in MODES 1, 2, and 3.

The Allowable Value for this trip is set below the full load operating value for steam pressure so as not to interfere with normal plant operation. However, the setting is high enough to provide an MSIS (Function 4) during an excessive steam demand event. An excessive steam demand event causes the RCS to cool down, resulting in a positive reactivity addition to the core.

MSIS limits this cooldown by isolating both steam generators if the pressure in either drops below the trip setpoint. An RPS trip on Steam Generator Pressure - Low is initiated simultaneously, using the same bistable. The Steam Generator Pressure - Low bistable output is also used in the EFAS logic (Function 7) to aid in determining if a steam generator is intact.

The Steam Generator Pressure - Low trip setpoint may be manually decreased as steam generator pressure is reduced. This prevents an RPS trip or MSIS actuation during controlled plant cooldown. The margin between actual pressurizer pressure and the trip setpoint must be maintained less than or equal to the specified value of 200 psia to ensure a reactor trip and MSIS will occur when required.

b. Containment Pressure - High

This LCO requires four channels of Containment Pressure - High to be OPERABLE in MODES 1, 2, and 3. The Containment Pressure - High signal is shared among the SIAS (Function 1), CIAS (Function 3), and MSIS (Function 4).

BASES

LCO (continued)

The Allowable Value for this trip is set high enough to allow for small pressure increases in containment expected during normal operation (i.e., plant heatup) and is not indicative of an abnormal condition. The setting is low enough to initiate the ESF Functions when an abnormal condition is indicated. This allows the ESF systems to perform as expected in the accident analyses to mitigate the consequences of the analyzed accidents.

5. <u>Recirculation Actuation Signal</u>

a. <u>Refueling Water Storage Tank Level - Low</u>

This LCO requires four channels of RWST Level - Low to be OPERABLE in MODES 1, 2, and 3.

The upper limit on the Allowable Value for this trip is set low enough to ensure RAS does not initiate before sufficient water is transferred to the containment sump. Premature recirculation could impair the reactivity control function of safety injection by limiting the amount of boron injection. Premature recirculation could also damage or disable the recirculation system if recirculation begins before the sump has enough water to prevent air entrainment in the suction. The lower limit on the RWST Level - Low trip Allowable Value is high enough to transfer suction to the containment sump prior to emptying the RWST.

6, 7 <u>Emergency Feedwater Actuation Signal SG #1 and SG #2 (EFAS-1 and EFAS-2)</u>

EFAS-1 is initiated to SG #1 by either a low steam generator level coincident with no low pressure trip present on SG #1 or by a low steam generator level coincident with a differential pressure between the two generators with the higher pressure in SG #1. EFAS-2 is similarly configured to feed SG #2.

BASES

LCO (continued)

The steam generator secondary differential pressure is used, in conjunction with a Steam Generator Pressure - Low input from each steam generator, as an input of the EFAS logic where it is used to determine if a generator is intact. The EFAS logic inhibits feeding a steam generator if a Steam Generator Pressure - Low condition exists in that generator and the pressure in that steam generator is less than the pressure in the other steam generator by the Steam Generator Pressure Difference (SGPD) - High setpoint.

The SGPD logic thus enables the feeding of a steam generator in the event that a plant cooldown causes a Steam Generator Pressure - Low condition, while inhibiting feeding the other (lower pressure) steam generator, which may be ruptured. The setpoint is high enough to allow for small pressure differences and normal instrumentation errors between the steam generator channels during normal operation.

The following LCO description applies to both EFAS signals.

a. Steam Generator Level - Low

This LCO requires four channels of Steam Generator Level - Low to be OPERABLE for each EFAS in MODES 1, 2, and 3.

The Steam Generator Level - Low EFAS input is derived from the Steam Generator Level - Low RPS bistable output. EFAS is thus initiated simultaneously with a reactor trip. The setpoint ensures at least a 20 minute inventory of water remains in the affected steam generator at reactor trip. Thus, EFAS is initiated well before steam generator inventory is challenged.

b. SG Pressure Difference - High (SG #1 > SG #2) or (SG #2 > SG #1)

This LCO requires four channels of SG Pressure Difference - High to be OPERABLE for each EFAS in MODES 1, 2, and 3.

The Allowable Value for this trip is high enough to allow for small pressure differences and normal instrumentation errors between the steam generator channels during normal operation without an actuation. The setting is low enough to detect and inhibit feeding of a ruptured steam generator in the event of an MSLB or FWLB, while permitting the feeding of the intact steam generator.

BASES

LCO (continued)

c. Steam Generator Pressure - Low

This LCO requires four channels of Steam Generator Pressure - Low to be OPERABLE for each EFAS in MODES 1, 2, and 3.

The Steam Generator Pressure - Low input is derived from the Steam Generator Pressure - Low RPS bistable output. This output is also used as an MSIS input.

The Allowable Value for this trip is set below the full load operating value for steam pressure so as not to interfere with normal plant operation. However, the setting is high enough to provide an MSIS (Function 4) during an excessive steam demand event. An excessive steam demand is one indicator of a potentially ruptured steam generator; thus, this EFAS input, in conjunction with the SGPD Function, prevents the feeding of a potentially ruptured steam generator.

The Steam Generator Pressure - Low trip setpoint may be manually decreased as steam generator pressure is reduced. This prevents an RPS trip or MSIS actuation during controlled plant cooldown. The margin between actual pressurizer pressure and the trip setpoint must be maintained less than or equal to the specified value of 200 psi to ensure that a reactor trip and MSIS will occur when required.

APPLICABILITY

In MODES 1, 2 and 3 there is sufficient energy in the primary and secondary systems to warrant automatic ESF System responses to:

- Close the main steam isolation valves to preclude a positive reactivity addition,
- Actuate emergency feedwater to preclude the loss of the steam generators as a heat sink (in the event the normal feedwater system is not available),
- Actuate ESF systems to prevent or limit the release of fission product radioactivity to the environment by isolating containment and limiting the containment pressure from exceeding the containment design pressure during a design basis LOCA or MSLB, and
- Actuate ESF systems to ensure sufficient borated inventory to permit adequate core cooling and reactivity control during a design basis LOCA or MSLB accident.

BASES

APPLICABILITY (continued)

In MODES 4, 5, and 6, automatic actuation of these Functions is not required because adequate time is available to evaluate plant conditions and respond by manually operating the ESF components if required, as addressed by LCO 3.3.6.

Several trips have operating bypasses, discussed in the preceding LCO section. The interlocks that allow these bypasses shall be OPERABLE whenever the RPS Function they support is OPERABLE.

ACTIONS

The most common causes of channel inoperability are outright failure or drift of the bistable or process module sufficient to exceed the tolerance allowed by the plant specific setpoint analysis. Typically, the drift is found to be small and results in a delay of actuation rather than a total loss of function. Determination of setpoint drift is generally made during the performance of a CHANNEL FUNCTIONAL TEST when the process instrument is set up for adjustment to bring it to within specification.

In the event a channel's trip setpoint is found nonconservative with respect to the Allowable Value, or the transmitter, instrument loop, signal processing electronics, or ESFAS bistable is found inoperable, then all affected Functions provided by that channel must be declared inoperable and the LCO Condition entered for the particular protection Function affected.

When the number of inoperable channels in a trip Function exceeds those specified in any related Condition associated with the same trip Function, then the plant is outside the safety analysis. Therefore, LCO 3.0.3 should be entered immediately, if applicable in the current MODE of operation.

A Note has been added to the ACTIONS. The Note has been added to clarify the application of the Completion Time rules. The Conditions of this Specification may be entered independently for each Function. The Completion Time for the inoperable channel of a Function will be tracked separately for each Function starting from the time the Condition was entered for that Function.

A.1 and A.2

Condition A applies to the failure of a single channel of one or more input parameters in the following ESFAS Functions:

1. Safety Injection Actuation Signal Containment Pressure - High
   Pressurizer Pressure - Low

BASES

ACTIONS (continued)

2. Containment Spray Actuation Signal Containment Pressure - High High Automatic SIAS

3. Containment Isolation Actuation Signal Containment Pressure - High Pressurizer Pressure - Low

4. Main Steam Isolation Signal Steam Generator Pressure - Low Containment Pressure - High

5. Recirculation Actuation Signal Refueling Water Storage Tank Level - Low

6. Emergency Feedwater Actuation Signal SG #1 (EFAS-1) Steam Generator Level - Low SG Pressure Difference - High Steam Generator Pressure - Low

7. Emergency Feedwater Actuation Signal SG #2 (EFAS-2) Steam Generator Level - Low SG Pressure Difference - High Steam Generator Pressure - Low

ESFAS coincidence logic is normally two-out-of-four.

If one ESFAS channel is inoperable, startup or power operation is allowed to continue, providing the inoperable channel is placed in bypass or trip within 1 hour (Required Action A.1).

The Completion Time of 1 hour allotted to restore, bypass, or trip the channel is sufficient to allow the operator to take all appropriate actions for the failed channel and still ensures that the risk involved in operating with the failed channel is acceptable.

The failed channel must be restored to OPERABLE status prior to entering MODE 2 following the next MODE 5 entry. With a channel bypassed, the coincidence logic is now in a two-out-of-three configuration. In this configuration, common cause failure of dependent channels cannot prevent trip. The Completion Time of prior to entering MODE 2 following the next MODE 5 entry is based on adequate channel to channel independence, which allows a two-out-of-three channel operation, since no single failure will cause or prevent a reactor trip.

BASES

ACTIONS (continued)

B.1

Condition B applies to the failure of two channels of one or more input parameters in the following ESFAS automatic trip Functions:

1. Safety Injection Actuation Signal Containment Pressure - High Pressurizer Pressure - Low

2. Containment Spray Actuation Signal Containment Pressure - High High Automatic SIAS

3. Containment Isolation Actuation Signal Containment Pressure - High Pressurizer Pressure - Low

4. Main Steam Isolation Signal Steam Generator Pressure - Low Containment Pressure - High

5. Recirculation Actuation Signal Refueling Water Storage Tank Level - Low

6. Emergency Feedwater Actuation Signal SG #1 (EFAS-1) Steam Generator Level - Low SG Pressure Difference - High Steam Generator Pressure - Low

7. Emergency Feedwater Actuation Signal SG #2 (EFAS-2) Steam Generator Level - Low SG Pressure Difference - High Steam Generator Pressure - Low

With two inoperable channels, power operation may continue, provided one inoperable channel is placed in bypass and the other channel is placed in trip within 1 hour. With one channel of protective instrumentation bypassed, the ESFAS Function is in two-out-of-three logic in the bypassed input parameter, but with another channel failed, the ESFAS may be operating with a two-out-of-two logic. This is outside the assumptions made in the analyses and should be corrected. To correct the problem, the second channel is placed in trip. This places the ESFAS Function in a one-out-of-two logic. If any of the other OPERABLE channels receives a trip signal, ESFAS actuation will occur.

BASES

ACTIONS (continued)

One of the two inoperable channels will need to be restored to OPERABLE status prior to the next required CHANNEL FUNCTIONAL TEST because channel surveillance testing on an OPERABLE channel requires that the OPERABLE channel be placed in bypass. However, it is not possible to bypass more than one ESFAS channel, and placing a second channel in trip will result in an ESFAS actuation. Therefore, if one ESFAS channel is in trip and a second channel is in bypass, a third inoperable channel would place the unit in LCO 3.0.3.

C.1, C.2.1, and C.2.2

Condition C applies to one automatic bypass removal channel inoperable. The only automatic bypass removal on an ESFAS is on the Pressurizer Pressure - Low signal. This bypass removal is shared with the RPS Pressurizer Pressure - Low bypass removal.

If the bypass removal channel for any operating bypass cannot be restored to OPERABLE status, the associated ESFAS channel may be considered OPERABLE only if the bypass is not in effect. Otherwise, the affected ESFAS channel must be declared inoperable, as in Condition A, and the bypass either removed or the bypass removal channel repaired. The Bases for the Required Actions and required Completion Times are consistent with Condition A.

D.1 and D.2

Otherwise, the affected ESFAS channels must be declared inoperable, as in Condition B, and either the bypass removed or the bypass removal channel repaired. The restoration of one affected bypassed automatic trip channel must be completed prior to the next CHANNEL FUNCTIONAL TEST or the plant must shut down per LCO 3.0.3, as explained in Condition B. Completion Times are consistent with Condition B.

BASES

ACTIONS (continued)

E.1 and E.2

If the Required Actions and associated Completion Times of Condition A, B, C, or D cannot be met, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 4 within [12] hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.3.5.1

Performance of the CHANNEL CHECK once every 12 hours ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the parameter indicated on one channel to a similar parameter on other channels. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value. Significant deviations between instrument channels could be an indication of excessive instrument drift in one of the channels or of something even more serious. CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

Agreement criteria are determined by the plant staff based on a combination of the channel instrument uncertainties, including indication and readability. If a channel is outside the criteria, it may be an indication that the sensor or the signal processing equipment has drifted outside its limit. If the channels are within the criteria, it is an indication that the channels are OPERABLE.

The Frequency, about once every shift, is based on operating experience that demonstrates channel failure is rare. Since the probability of two random failures in redundant channels in any 12 hour period is low, the CHANNEL CHECK minimizes the chance of loss of protective function due to failure of redundant channels. The CHANNEL CHECK supplements less formal, but more frequent, checks of channel OPERABILITY during normal operational use of displays associated with the LCO required channels.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.5.2

A CHANNEL FUNCTIONAL TEST is performed every 92 days to ensure the entire channel will perform its intended function when needed. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

The CHANNEL FUNCTIONAL TEST is part of an overlapping test sequence similar to that employed in the RPS. This sequence, consisting of SR 3.3.5.2, SR 3.3.6.1, and SR 3.3.6.2, tests the entire ESFAS from the bistable input through the actuation of the individual subgroup relays. These overlapping tests are described in Reference 1. SR 3.3.5.2 and SR 3.3.6.1 are normally performed together and in conjunction with ESFAS testing. SR 3.3.6.2 verifies that the subgroup relays are capable of actuating their respective ESF components when de-energized.

These tests verify that the ESFAS is capable of performing its intended function, from bistable input through the actuated components.
SRs 3.3.6.1 and 3.3.6.2 are addressed in LCO 3.3.6. SR 3.3.5.2 includes bistable tests.

A test signal is superimposed on the input in one channel at a time to verify that the bistable trips within the specified tolerance around the setpoint. This is done with the affected RPS trip channel bypassed. Any setpoint adjustment shall be consistent with the assumptions of the current plant specific setpoint analysis.

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the surveillance interval extension analysis. The requirements for this review are outlined in Reference [9].

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.5.3

CHANNEL CALIBRATION is a complete check of the instrument channel including the detector and the bypass removal functions. The Surveillance verifies that the channel responds to a measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drift between successive calibrations to ensure that the channel remains operational between successive surveillances. CHANNEL CALIBRATIONS must be performed consistent with the plant specific setpoint analysis.

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the surveillance interval extension analysis. The requirements for this review are outlined in Reference [9].

The [18] month Frequency is based on the need to perform this Surveillance under the conditions that apply during a plant outage and the potential for an unplanned transient if the Surveillance were performed with the reactor at power.

SR 3.3.5.4

This Surveillance ensures that the train actuation response times are within the maximum values assumed in the safety analyses.

Response time testing acceptance criteria are included in Reference 10.

-----------------------------------REVIEWER'S NOTE-----------------------------------
Applicable portions of the following TS Bases are applicable to plants adopting CEOG Topical Report CE NPSD-1167-1, "Elimination of Pressure Sensor Response Time Testing Requirements."

Response time may be verified by any series of sequential, overlapping or total channel measurements, including allocated sensor response time, such that the response time is verified. Allocations for sensor response times may be obtained from records of test results, vendor test data, or vendor engineering specifications. Topical Report CE NPSD-1167-A,

BASES

SURVEILLANCE REQUIREMENTS (continued)

"Elimination of Pressure Sensor Response Time Testing Requirements," (Ref. 11) provides the basis and methodology for using allocated sensor response times in the overall verification of the channel response time for specific sensors identified in the Topical Report. Response time verification for other sensor types must be demonstrated by test. The allocation of sensor response times must be verified prior to placing a new component in operation and reverified after maintenance that may adversely affect the sensor response time.

ESF RESPONSE TIME tests are conducted on a STAGGERED TEST BASIS of once every [18] months. The [18] month Frequency is consistent with the typical industry refueling cycle and is based upon plant operating experience, which shows that random failures of instrumentation components causing serious response time degradation, but not channel failure, are infrequent occurrences.

SR 3.3.5.5

SR 3.3.5.5 is a CHANNEL FUNCTIONAL TEST similar to SR 3.3.5.2, except SR 3.3.5.5 is performed within 92 days prior to startup and is only applicable to bypass functions. Since the Pressurizer Pressure - Low bypass is identical for both the RPS and ESFAS, this is the same Surveillance performed for the RPS in SR 3.3.1.13. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

The CHANNEL FUNCTIONAL TEST for proper operation of the bypass permissives is critical during plant heatups because the bypasses may be in place prior to entering MODE 3 but must be removed at the appropriate points during plant startup to enable the ESFAS Function. Consequently, just prior to startup is the appropriate time to verify bypass function OPERABILITY. Once the bypasses are removed, the bypasses must not fail in such a way that the associated ESFAS Function is inappropriately bypassed. This feature is verified by SR 3.3.5.2.

The allowance to conduct this test with 92 days of startup is based on the reliability analysis presented in topical report CEN-327, "RPS/ESFAS Extended Test Interval Evaluation" (Ref. 9).

BASES

REFERENCES

1. FSAR, Section [7.3].
2. 10 CFR 50, Appendix A.
3. NRC Safety Evaluation Report.
4. IEEE Standard 279-1971.
5. FSAR, Chapter [15].
6. 10 CFR 50.49.
7. "Plant Protection System Selection of Trip Setpoint Values."
8. FSAR, Section [7.2].
9. CEN-327, May 1986, including Supplement 1, March 1989.
10. Response Time Testing Acceptance Criteria.
11. CEOG Topical Report CE NPSD-1167-A, "Elimination of Pressure Sensor Response Time Testing Requirements."

B 3.3 INSTRUMENTATION

B 3.3.6 Engineered Safety Features Actuation System (ESFAS) Logic and Manual Trip (Digital)

BASES

BACKGROUND

The ESFAS initiates necessary safety systems, based upon the values of selected unit parameters, to protect against violating core design limits and the Reactor Coolant System (RCS) pressure boundary during anticipated operational occurrences (AOOs) and ensures acceptable consequences during accidents.

The ESFAS contains devices and circuitry that generate the following signals when monitored variables reach levels that are indicative of conditions requiring protective action:

1. Safety Injection Actuation Signal (SIAS),
2. Containment Isolation Actuation Signal (CIAS),
3. Containment Cooling Actuation Signal (CCAS),
4. Recirculation Actuation Signal (RAS),
5. Containment Spray Actuation Signal (CSAS),
6. Main Steam Isolation Signal (MSIS),
7. Emergency Feedwater Actuation Signal SG #1 (EFAS-1), and
8. Emergency Feedwater Actuation Signal SG #2 (EFAS-2).

Equipment actuated by each of the above signals is identified in the FSAR (Ref. 1).

Each of the above ESFAS instrumentation systems is segmented into three interconnected modules. These modules are:

- Measurement channels,
- Bistable trip units, and

BASES

BACKGROUND (continued)

- ESFAS Logic:
  - Matrix Logic,
  - Initiation Logic (trip paths), and
  - Actuation Logic.

This LCO addresses ESFAS Logic. Bistables and measurement channels are addressed in LCO 3.3.5, "Engineered Safety Features Actuation System (ESFAS) Instrumentation."

The role of the measurement channels and bistables is described in LCO 3.3.5. The role of the ESFAS Logic is described below.

ESFAS Logic

The ESFAS Logic, consisting of Matrix, Initiation and Actuation Logic, employs a scheme that provides an ESF actuation of both trains when bistables in any two of the four channels sense the same input parameter trip. This is called a two-out-of-four trip logic.

Bistable relay contact outputs from the four channels are configured into six Matrix Logics. Each Matrix Logic checks for a coincident trip in the same parameter in two bistable channels. The matrices are designated the AB, AC, AD, BC, BD, and CD matrices, to reflect the bistable channels being monitored. Each Matrix Logic contains four normally energized matrix relays. When a coincidence is detected in the two channels being monitored by the Matrix Logic, all four matrix relays de-energize.

The matrix relay contacts are arranged into trip paths, with one relay contact from each matrix relay in each of the four trip paths. Each trip path controls two initiation relays. Each of the two initiation relays in each trip path controls contacts in the Actuation Logic for one train of ESF.

Each of the two channels of Actuation Logic, mounted in the Auxiliary Relay Cabinets (ARCs), is responsible for actuating one train of ESF equipment. Each ESF Function has separate Actuation Logic in each ARC.

BASES

BACKGROUND (continued)

The contacts from the Initiation Logic are configured in a selective two-out-of-four logic in the Actuation Logic, similar to the configuration employed by the RPS in the RTCBs. This logic controls ARC mounted subgroup relays, which are normally energized. Contacts from these relays, when de-energized, actuate specific ESF equipment.

When a coincidence occurs in two ESFAS channels, all four matrix relays in the affected matrix will de-energize. This, in turn, will de-energize all eight initiation relays, four used in each Actuation Logic.

Matrix Logic refers to the matrix power supplies, trip channel bypass contacts, and interconnecting matrix wiring between bistable relay cards, up to but not including the matrix relays. Matrix contacts on the bistable relay cards are excluded from the Matrix Logic definition, since they are addressed as part of the measurement channel.

Initiation Logic consists of the trip path power source, matrix relays and their associated contacts, all interconnecting wiring, and the initiation relays.

Actuation Logic consists of all circuitry housed within the ARCs used to actuate the ESF Function, excluding the subgroup relays, and interconnecting wiring to the initiation relay contacts mounted in the PPS cabinet.

The subgroup relays are actuated by the ESFAS Logic. Each ESFAS Function typically employs several subgroup relays, with each subgroup relay responsible for actuating one or more components in the ESFAS Function. Subgroup relays and their contacts are considered part of the actuated equipment and are addressed under the applicable LCO for this equipment.

It is possible to change the two-out-of-four ESFAS Logic to two-out-of-three logic for a given input parameter in one channel at a time by trip channel bypassing select portions of the Matrix Logic. Trip channel bypassing a bistable effectively shorts the bistable relay contacts in the three matrices associated with that channel. Thus, the bistables will function normally, producing normal trip indication and annunciation, but ESFAS actuation will not occur since the bypassed channel is effectively removed from the coincidence logic. Trip channel bypassing can be

BASES

BACKGROUND (continued)

simultaneously performed on any number of parameters in any number of channels, providing each parameter is bypassed in only one channel at a time. An interlock prevents simultaneous trip channel bypassing of the same parameter in more than one channel. Trip channel bypassing is normally employed during maintenance or testing. Trip channel bypassing is addressed in LCO 3.3.5.

Manual ESFAS initiation capability is provided to permit the operator to manually actuate an ESF System when necessary.

Two sets of two push buttons (located in the control room) for each ESF Function are provided, and each set actuates both trains. Each Manual Trip push button opens one trip path, de-energizing one set of two initiation relays, one affecting each train of ESF. Initiation relay contacts are arranged in a selective two-out-of-four configuration in the Actuation Logic. By arranging the push buttons in two sets of two, such that both push buttons in a set must be depressed, it is possible to ensure that Manual Trip will not be prevented in the event of a single random failure. Each set of two push buttons is designated a single channel in this LCO.

APPLICABLE SAFETY ANALYSES

Each of the analyzed accidents can be detected by one or more ESFAS Functions. One of the ESFAS Functions is the primary actuation signal for that accident. An ESFAS Function may be the primary actuation signal for more than one type of accident. An ESFAS Function may also be a secondary, or backup, actuation signal for one or more other accidents.

ESFAS Functions are as follows:

1. Safety Injection Actuation Signal

   SIAS ensures acceptable consequences during large break loss of coolant accidents (LOCAs), small break LOCAs, control element assembly ejection accidents, and main steam line breaks (MSLBs) inside containment. To provide the required protection, either a high containment pressure or a low pressurizer pressure signal will initiate SIAS. SIAS initiates the Emergency Core Cooling Systems (ECCS) and performs several other Functions, such as initiating a containment cooling actuation, initiating control room isolation, and starting the diesel generators.

BASES

APPLICABLE SAFETY ANALYSES (continued)

2. Containment Isolation Actuation Signal

CIAS ensures acceptable mitigating actions during large and small break LOCAs and during MSLBs or feedwater line breaks (FWLBs) either inside or outside containment. CIAS is initiated by low pressurizer pressure or high containment pressure.

3. Containment Cooling Actuation Signal

CCAS mitigates containment overpressurization when required by either a manual CCAS actuation or an automatic SIAS Function. This Function is not employed by all plants.

4. Recirculation Actuation Signal

At the end of the injection phase of a LOCA, the refueling water storage tank (RWST) will be nearly empty. Continued cooling must be provided by the ECCS to remove decay heat. The source of water for the ECCS pumps is automatically switched to the containment recirculation sump. Switchover from RWST to containment sump must occur before the RWST empties to prevent damage to the ECCS pumps and a loss of core cooling capability. For similar reasons, switchover must not occur before there is sufficient water in the containment sump to support pump suction. Furthermore, early switchover must not occur to ensure sufficient borated water is injected from the RWST to ensure the reactor remains shut down in the recirculation mode. An RWST Level - Low signal initiates the RAS.

5. Containment Spray Actuation Signal

CSAS actuates containment spray, preventing containment overpressurization during large break LOCAs, small break LOCAs, and MSLBs or FWLBs inside containment. CSAS is initiated by high high containment pressure and an SIAS. This configuration reduces the likelihood of inadvertent containment spray.

BASES

APPLICABLE SAFETY ANALYSES (continued)

6. Main Steam Isolation Signal

MSIS ensures acceptable consequences during an MSLB or FWLB (between the steam generator and the main feedwater check valve) either inside or outside containment. MSIS isolates both steam generators if either generator indicates a low pressure condition or if a high containment pressure condition exists. This prevents an excessive rate of heat extraction and subsequent cooldown of the RCS during these events.

7, 8. Emergency Feedwater Actuation Signal

EFAS consists of two steam generator (SG) specific signals (EFAS-1 and EFAS-2). EFAS-1 initiates emergency feed to SG #1, and EFAS-2 initiates emergency feed to SG #2.

EFAS maintains a steam generator heat sink during a steam generator tube rupture event and an MSLB or FWLB event either inside or outside containment.

Low steam generator water level initiates emergency feed to the affected steam generator, providing the generator is not identified (by the circuitry) as faulted (an MSLB or FWLB).

EFAS logic includes steam generator specific inputs from the Steam Generator Pressure - Low bistable comparator (also used in MSIS) and the SG Pressure Difference - High (SG #1 > SG #2 or SG #2 > SG #1, bistable comparators) to determine if a rupture in either generator has occurred.

Rupture is assumed if the affected generator has a low pressure condition, unless that generator is significantly higher in pressure than the other generator.

This latter feature allows feeding the intact steam generator even if both are below the MSIS setpoint, while preventing the ruptured generator from being fed. Not feeding a ruptured generator prevents containment overpressurization during the analyzed events.

The ESFAS satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO

The LCO requires all channel components necessary to provide an ESFAS actuation to be OPERABLE.

The requirements for each Function are listed below. The reasons for the applicable MODES for each Function are addressed under APPLICABILITY.

1. Safety Injection Actuation Signal

   Automatic SIAS is required to initiate CCAS and CSAS. Automatic SIAS occurs in Pressurizer Pressure - Low or Containment Pressure - High and is explained in Bases 3.3.5.

   a. Manual Trip

      This LCO requires two channels of SIAS Manual Trip to be OPERABLE in MODES 1, 2, 3, and 4.

   b. Matrix Logic

      This LCO requires six channels of SIAS Matrix Logic to be OPERABLE in MODES 1, 2, and 3.

   c. Initiation Logic

      This LCO requires four channels of SIAS Initiation Logic to be OPERABLE in MODES 1, 2, 3, and 4.

   d. Actuation Logic

      This LCO requires two channels of SIAS Actuation Logic to be OPERABLE in MODES 1, 2, 3, and 4.

2. Containment Isolation Actuation Signal

   For plants where the SIAS and CIAS are actuated on Pressurizer Pressure - Low or Containment Pressure - High, the SIAS and CIAS share the same input channels, bistables, and matrices and matrix relays. The remainder of the initiation channels, the manual channels, and the Actuation Logic are separate. Since their applicability is also the same, they have identical actions.

   a. Manual Trip

      This LCO requires two channels of CIAS Manual Trip to be OPERABLE in MODES 1, 2, 3, and 4.

BASES

LCO (continued)

b. Matrix Logic

This LCO requires six channels of CIAS Matrix Logic to be OPERABLE in MODES 1, 2, and 3.

c. Initiation Logic

This LCO requires four channels of CIAS Initiation Logic to be OPERABLE in MODES 1, 2, 3, and 4.

d. Actuation Logic

This LCO requires two channels of CIAS Actuation Logic to be OPERABLE in MODES 1, 2, 3, and 4.

3. Containment Cooling Actuation Signal

For plants employing a separate CCAS signal, the CCAS Function can be automatically actuated on an SIAS. It can also be manually actuated using two channels of CCAS push buttons, configured similarly to all other ESFAS Manual Trips. CCAS therefore shares the SIAS sensor channels, bistables, coincidence matrices, and matrix relays. It has separate manual channels and Actuation Logic.

a. Manual Trip

This LCO requires two channels of CCAS Manual Trip to be OPERABLE in MODES 1, 2, 3, and 4.

b. Initiation Logic

This LCO requires four channels of CCAS Initiation Logic to be OPERABLE in MODES 1, 2, 3, and 4.

c. Actuation Logic

This LCO requires two channels of CCAS Actuation Logic to be OPERABLE in MODES 1, 2, 3, and 4.

BASES

LCO (continued)

4. Recirculation Actuation Signal

   a. Manual Trip

      This LCO requires two channels of RAS Manual Trip to be OPERABLE in MODES 1, 2, 3, and 4.

   b. Matrix Logic

      This LCO requires six channels of RAS Matrix Logic to be OPERABLE in MODES 1, 2, and 3.

   c. Initiation Logic

      This LCO requires four channels of RAS Initiation Logic to be OPERABLE in MODES 1, 2, 3, and 4.

   d. Actuation Logic

      This LCO requires two channels of RAS Actuation Logic to be OPERABLE in MODES 1, 2, 3, and 4.

5. Containment Spray Actuation Signal

   CSAS is initiated either manually or automatically. For an automatic actuation it is necessary to have a Containment Pressure - High High signal, coincident with an SIAS. The SIAS requirement should always be satisfied on a legitimate CSAS, since the Containment Pressure - High signal used in the SIAS will initiate before the Containment Pressure - High High input signal to CSAS. This ensures that a CSAS will not initiate unless required.

   a. Manual Trip

      This LCO requires two channels of CSAS Manual Trip to be OPERABLE in MODES 1, 2, and 3.

   b. Automatic SIAS (Function 1)

      This LCO requires four channels of Automatic SIAS input to CSAS to be OPERABLE in MODES 1, 2, and 3.

      The Automatic SIAS occurs on Pressurizer Pressure - Low or Containment Pressure - High and is explained above.

BASES

LCO (continued)

c. Matrix Logic

This LCO requires six channels of CSAS Matrix Logic to be OPERABLE in MODES 1, 2, and 3.

d. Initiation Logic

This LCO requires four channels of CSAS Initiation Logic to be OPERABLE in MODES 1, 2, and 3.

e. Actuation Logic

This LCO requires two channels of CSAS Actuation Logic to be OPERABLE in MODES 1, 2, and 3.

6. Main Steam Isolation Signal

a. Manual Trip

This LCO requires two channels of MSIS Manual Trip to be OPERABLE in MODES 1, 2, and 3.

b. Matrix Logic

This LCO requires six channels of MSIS Matrix Logic to be OPERABLE in MODES 1, 2, and 3.

c. Initiation Logic

This LCO requires four channels of MSIS Initiation Logic to be OPERABLE in MODES 1, 2, and 3.

d. Actuation Logic

This LCO requires two channels of MSIS Actuation Logic to be OPERABLE in MODES 1, 2, and 3.

7. Emergency Feedwater Actuation Signal SG #1 (EFAS-1)

EFAS-1 is initiated either by a low steam generator level coincident with no low pressure trip present on SG #1 or by a low steam generator level coincident with a differential pressure between the two generators with the higher pressure in SG #1.

BASES

LCO (continued)

The steam generator secondary differential pressure is used, in conjunction with a Steam Generator Pressure - Low input from each steam generator, as an input of the EFAS logic where it is used to determine if a generator is intact. The EFAS logic inhibits feeding a steam generator if a Steam Generator Pressure - Low condition exists in that generator and the pressure in that steam generator is less than the Steam Generator Pressure Difference (SGPD) - High setpoint pressure.

The SGPD logic thus enables the feeding of a steam generator in the event that a plant cooldown causes a Steam Generator Pressure - Low condition, while inhibiting feeding the other (lower pressure) steam generator, which may be ruptured. The setpoint is high enough to allow for small pressure differences and normal instrumentation errors between the steam generator channels during normal operation.

a. Manual Trip

This LCO requires two channels of Manual Trip to be OPERABLE in MODES 1, 2, and 3.

b. Matrix Logic

This LCO requires six channels of Matrix Logic to be OPERABLE in MODES 1, 2, and 3.

c. Initiation Logic

This LCO requires four channels of Initiation Logic to be OPERABLE in MODES 1, 2, and 3.

d. Actuation Logic

This LCO requires one channel of Actuation Logic to be OPERABLE in MODES 1, 2, and 3.

8. Emergency Feedwater Actuation Signal SG #2 (EFAS-2)

EFAS-2 is initiated either by a low steam generator level coincident with no low pressure trip present on SG #2 or by a low steam generator level coincident with a differential pressure between the two generators with the higher pressure in SG #2.

BASES

LCO (continued)

The steam generator secondary differential pressure is used, in conjunction with a Steam Generator Pressure - Low input from each steam generator, as an input of the EFAS Logic where it is used to determine if a generator is intact. The EFAS Logic inhibits feeding a steam generator if a Steam Generator Pressure - Low condition exists in that generator and the pressure in that steam generator is less than the SGPD - High setpoint pressure.

The SGPD logic thus enables the feeding of a steam generator in the event that a plant cooldown causes a Steam Generator Pressure - Low condition, while inhibiting feeding the other (lower pressure) steam generator, which may be ruptured. The setpoint is high enough to allow for small pressure differences and normal instrumentation errors between the steam generator channels during normal operation.

a. <u>Manual Trip</u>

   This LCO requires two channels of Manual Trip to be OPERABLE in MODES 1, 2, and 3.

b. <u>Matrix Logic</u>

   This LCO requires six channels of Matrix Logic to be OPERABLE in MODES 1, 2, and 3.

c. <u>Initiation Logic</u>

   This LCO requires four channels of Initiation Logic to be OPERABLE in MODES 1, 2, and 3.

d. <u>Actuation Logic</u>

   This LCO requires one channel of Actuation Logic to be OPERABLE in MODES 1, 2, and 3.

APPLICABILITY

In MODES 1, 2 and 3, there is sufficient energy in the primary and secondary systems to warrant automatic ESF System responses to:

- Close the main steam isolation valves to preclude a positive reactivity addition,

BASES

APPLICABILITY (continued)

- Actuate emergency feedwater to preclude the loss of the steam generators as a heat sink (in the event the normal feedwater system is not available),

- Actuate ESF systems to prevent or limit the release of fission product radioactivity to the environment by isolating containment and limiting the containment pressure from exceeding the containment design pressure during a design basis LOCA or MSLB, and

- Actuate ESF systems to ensure sufficient borated inventory to permit adequate core cooling and reactivity control during a design basis LOCA or MSLB accident.

In MODES 4, 5, and 6, automatic actuation of these Functions is not required because adequate time is available to evaluate plant conditions and respond by manually operating the ESF components if required.

ESFAS Manual Trip capability is required in MODE 4 for SIAS, CIAS, CCAS, and RAS even though automatic actuation is not required. Because of the large number of components actuated by these Functions, ESFAS actuation is simplified by the use of the Manual Trip push buttons.

CSAS, MSIS, and EFAS have relatively few components, which can be actuated individually if required in MODE 4, and the systems may be disabled or reconfigured, making system level Manual Trip impossible and unnecessary.

The ESFAS logic must be OPERABLE in the same MODES as the automatic and Manual Trip. In MODE 4, only the portion of the ESFAS logic responsible for the required Manual Trip must be OPERABLE.

In MODES 5 and 6, the systems initiated by ESFAS are either reconfigured or disabled for shutdown cooling operation. Accidents in these MODES are slow to develop and would be mitigated by manual operation of individual components.

ACTIONS

When the number of inoperable channels in a trip Function exceeds those specified in any related Condition associated with the same trip Function, then the plant is outside the safety analysis. Therefore, LCO 3.0.3 should be entered immediately, if applicable in the current MODE of operation.

BASES

ACTIONS (continued)

A Note has been added to the ACTIONS to clarify the application of the Completion Time rules. The Conditions of this Specification may be entered independently for each Function. The Completion Time for the inoperable channel of a Function will be tracked separately for each Function, starting from the time the Condition was entered for that Function.

A.1

Condition A applies if one Matrix Logic channel is inoperable. Since matrix power supplies in a given matrix (e.g., AB, BC, etc.) are common to all ESFAS Functions, a single power supply failure may affect more than one matrix.

Failures of individual bistables and their relays are considered measurement channel failures. This section describes failures of the Matrix Logic not addressed in the above, such as the failure of matrix relay power supplies, or the failure of the trip channel bypass contact in the bypass condition. Loss of a single vital bus will de-energize one of the two power supplies in each of three matrices. This will result in two initiation circuits de-energizing, reducing the ESFAS Actuation Logic to a one-out-of-two logic in both trains.

This Condition has been modified by a Note stating that for the purposes of this LCO, de-energizing up to three matrix power supplies due to a single failure, such as loss of a vital instrument bus, is to be treated as a single matrix channel failure, providing the affected matrix relays de-energize as designed. Although each of the six matrices within an ESFAS Function uses separate power supplies, the matrices for the different ESFAS Functions share power supplies. Thus, failure of a matrix power supply may force entry into the Condition specified for each of the affected ESFAS Functions.

The channel must be restored to OPERABLE status within 48 hours. This provides the operator with time to take appropriate actions and still ensures that any risk involved in operating with a failed channel is acceptable. Operating experience has demonstrated that the probability of a random failure of a second Matrix Logic channel is low during any given 48 hour period. If the channel cannot be restored to OPERABLE status with 48 hours, Condition E is entered.

BASES

ACTIONS (continued)

B.1

Condition B applies to one Manual Trip or Initiation Logic channel inoperable.

The channel must be restored to OPERABLE status within 48 hours. Operating experience has demonstrated that the probability of a random failure in a second channel is low during any given 48 hour period.

Failure of a single Initiation Logic channel may open one contact affecting both Actuation Logic channels. For the purposes of this Specification, the Actuation Logic is not inoperable. This prevents the need to enter LCO 3.0.3 in the event of an Initiation Logic channel failure. The Actions differ from those involving one RPS manual channel inoperable, because in the case of the RPS, opening RTCBs can be easily performed and verified. Opening an initiation relay contact is more difficult to verify, and subsequent shorting of the contact is always possible.

C.1 and C.2

Condition C applies to the failure of both Initiation Logic channels affecting the same trip leg.

In this case, the Actuation Logic channels are not inoperable, since they are in one-out-of-two logic and capable of performing as required. This obviates the need to enter LCO 3.0.3 in the event of a matrix or vital bus power failure.

Both Initiation Logic channels in the same trip leg will de-energize if a matrix power supply or vital instrument bus is lost. This will open the Actuation Logic contacts, satisfying the Required Action to open at least one set of contacts in the affected trip leg. Indefinite operation in this condition is prohibited because of the difficulty of ensuring the contacts remain open under all conditions. Thus, the channel must be restored to OPERABLE status within 48 hours. This provides the operator with time to take appropriate actions and still ensures that any risk involved in operating with a failed channel is acceptable. Operating experience has demonstrated that the probability of a random failure of a second channel is low during any given 48 hour period. If the channel cannot be restored to OPERABLE status with 48 hours, Condition E is entered.

BASES

ACTIONS (continued)

Of greater concern is the failure of the initiation circuit in a nontrip condition, e.g., due to two initiation relay failures. With one failed, there is still the redundant contact in the trip leg of each Actuation Logic. With both failed in a nontrip condition, the ESFAS Function is lost in the affected train. To prevent this, immediate opening of at least one contact in the affected trip leg is required. If the required contact has not opened, as indicated by annunciation or trip leg current lamps, Manual Trip of the affected trip leg contacts may be attempted. Caution must be exercised, since depressing the wrong ESFAS push buttons may result in an ESFAS actuation.

D.1

Condition D applies to Actuation Logic.

With one Actuation Logic channel inoperable, automatic actuation of one train of ESF may be inhibited. The remaining train provides adequate protection in the event of Design Basis Accidents, but the single failure criterion may be violated. For this reason operation in this condition is restricted.

The channel must be restored to OPERABLE status within 48 hours. Operating experience has demonstrated that the probability of a random failure in the Actuation Logic of the second train is low during a given 48 hour period.

Failure of a single Initiation Logic channel, matrix channel power supply, or vital instrument bus may open one or both contacts in the same trip leg in both Actuation Logic channels. For the purposes of this Specification, the Actuation Logic is not inoperable. This obviates the need to enter LCO 3.0.3 in the event of a vital bus, matrix, or initiation channel failure.

Required Action D.1 is modified by a Note to indicate that one channel of Actuation Logic may be bypassed for up to 1 hour for Surveillance, provided the other channel is OPERABLE.

This allows performance of a PPS CHANNEL FUNCTIONAL TEST on an OPERABLE ESFAS train without generating an ESFAS actuation in the inoperable train.

BASES

ACTIONS (continued)

E.1 and E.2

If two associated Actuation Logic channels are inoperable, or if the Required Actions and associated Completion Times of Conditions for CSAS, MSIS, or EFAS cannot be met, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 4 within [12] hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

F.1 and F.2

If two associated Actuation Logic channels are inoperable, or if the Required Actions and associated Completion Times for SIAS, CIAS, RAS, or CCAS are not met, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 5 within 36 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.3.6.1

A CHANNEL FUNCTIONAL TEST is performed every [92] days to ensure the entire channel will perform its intended function when needed. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The CHANNEL FUNCTIONAL TEST is part of an overlapping test sequence similar to that employed in the RPS. This sequence, consisting of SR 3.3.5.2, SR 3.3.6.1, and SR 3.3.6.2, tests the entire ESFAS from the bistable input through the actuation of the individual subgroup relays. These overlapping tests are described in Reference 1. SR 3.3.5.2 and SR 3.3.6.1 are normally performed together and in conjunction with ESFAS testing. SR 3.3.6.2 verifies that the subgroup relays are capable of actuating their respective ESF components when de-energized.

These tests verify that the ESFAS is capable of performing its intended function, from bistable input through the actuated components. SR 3.3.5.2 is addressed in LCO 3.3.5. SR 3.3.6.1 includes Matrix Logic tests and trip path (Initiation Logic) tests.

Matrix Logic Tests

These tests are performed one matrix at a time. They verify that a coincidence in the two input channels for each function removes power to the matrix relays. During testing, power is applied to the matrix relay test coils, preventing the matrix relay contacts from assuming their energized state. The Matrix Logic tests will detect any short circuits around the bistable contacts in the coincidence logic, such as may be caused by faulty bistable relay or trip channel bypass contacts.

Trip Path (Initiation Logic) Tests

These tests are similar to the Matrix Logic tests, except that test power is withheld from one matrix relay at a time, allowing the initiation circuit to de-energize, opening one contact in each Actuation Logic channel.

The initiation circuit lockout relay must be reset (except for EFAS, which lacks initiation circuit lockout relays) prior to testing the other three initiation circuits, or an ESFAS actuation may result.

Automatic Actuation Logic operation is verified during Initiation Logic testing by verifying that current is interrupted in each trip leg in the selective two-out-of-four actuation circuit logic whenever the initiation relay is de-energized. A Note is added to indicate that testing of Actuation Logic shall include verification of the proper operation of each initiation relay.

The Frequency of [92] days is based on the reliability analysis presented in topical report CEN-327, "RPS/ESFAS Extended Test Interval Evaluation" (Ref. 2).

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.6.2

Individual ESFAS subgroup relays must also be tested, one at a time, to verify the individual ESFAS components will actuate when required. Proper operation of the individual subgroup relays is verified by de-energizing these relays one at a time using an ARC mounted test circuit. Proper operation of each component actuated by the individual relays is thus verified without the need to actuate the entire ESFAS function.

The 184 day Frequency is based on operating experience and ensures individual relay problems can be detected within this time frame. Considering the large number of similar relays in the ARC, and the similarity in their use, a large test sample can be assembled to verify the validity of this Frequency. The actual justification is based on CEN-403, "Relaxation of Surveillance Test Interval for ESFAS Subgroup Relay Testing" (Ref. 3).

Some components cannot be tested at power since their actuation might lead to plant trip or equipment damage. Reference 1 lists those relays exempt from testing at power, with an explanation of the reason for each exception. Relays not tested at power must be tested in accordance with the Note to this SR.

SR 3.3.6.3

A CHANNEL FUNCTIONAL TEST is performed on the manual ESFAS actuation circuitry, de-energizing relays and providing manual actuation of the function. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

This test verifies that the trip push buttons are capable of opening contacts in the Actuation Logic as designed. The [18] month Frequency is based on the need to perform this Surveillance under the conditions that apply during a plant outage and the potential for an unplanned transient if the Surveillance were performed with the reactor at power. Operating experience has shown these components usually pass the Surveillance when performed at a Frequency of once every [18] months.

BASES

REFERENCES	1.	FSAR, Section [7.3].
	2.	CEN-327, May 1986, including Supplement 1, March 1989.
	3.	CEN-403.

B 3.3 INSTRUMENTATION

B 3.3.7 Diesel Generator (DG) - Loss of Voltage Start (LOVS) (Digital)

BASES

BACKGROUND

The DGs provide a source of emergency power when offsite power is either unavailable or insufficiently stable to allow safe unit operation. Undervoltage protection will generate a LOVS in the event a Loss of Voltage or Degraded Voltage condition occurs. There are two LOVS Functions for each 4.16 kV vital bus.

Four undervoltage relays with inverse time characteristics are provided on each 4.16 kV Class 1E instrument bus for the purpose of detecting a sustained undervoltage condition or a loss of bus voltage. The relays are combined in a two-out-of-four logic to generate a LOVS if the voltage is below 75% for a short time or below 90% for a long time. The LOVS initiated actions are described in "Onsite Power Systems" (Ref. 1).

<u>Trip Setpoints and Allowable Values</u>

The trip setpoints and Allowable Values are based on the analytical limits presented in "Accident Analysis," Reference 2. The selection of these trip setpoints is such that adequate protection is provided when all sensor and processing time delays are taken into account. To allow for calibration tolerances, instrumentation uncertainties, and instrument drift, Allowable Values specified in SR 3.3.7.3 are conservatively adjusted with respect to the analytical limits. A detailed description of the methodology used to calculate the trip setpoints, including their explicit uncertainties, is provided in Reference 3. The actual nominal trip setpoint is normally still more conservative than that required by the plant specific setpoint calculations. If the measured trip setpoint does not exceed the documented Surveillance acceptance criteria, the undervoltage relay is considered OPERABLE.

Setpoints in accordance with the Allowable Values will ensure that the consequences of accidents will be acceptable, providing the plant is operated from within the LCOs at the onset of the accident and the equipment functions as designed.

BASES

BACKGROUND (continued)

The undervoltage protection scheme has been designed to protect the plant from spurious trips caused by the offsite power source. This is made possible by the inverse voltage time characteristics of the relays used. A complete loss of offsite power will result in approximately a 1 second delay in LOVS actuation. The DG starts and is available to accept loads within a 10 second time interval on the Engineered Safety Features Actuation System (ESFAS) or LOVS. Emergency power is established within the maximum time delay assumed for each event analyzed in the accident analysis (Ref. 2).

Since there are four protective channels in a two-out-of-four trip logic for each division of the 4.16 kV power supply, no single failure will cause or prevent protective system actuation. This arrangement meets IEEE Standard 279-1971 criteria (Ref. 4).

APPLICABLE SAFETY ANALYSES

The DG - LOVS is required for Engineered Safety Features (ESF) systems to function in any accident with a loss of offsite power. Its design basis is that of the ESFAS.

Accident analyses credit the loading of the DG based on a loss of offsite power during a loss of coolant accident. The actual DG start has historically been associated with the ESFAS actuation. The diesel loading has been included in the delay time associated with each safety system component requiring DG supplied power following a loss of offsite power. The analysis assumes a nonmechanistic DG loading, which does not explicitly account for each individual component of the loss of power detection and subsequent actions. This delay time includes contributions from the DG start, DG loading, and Safety Injection System component actuation. The response of the DG to a loss of power must be demonstrated to fall within this analysis response time when including the contributions of all portions of the delay.

The required channels of LOVS, in conjunction with the ESF systems powered from the DGs, provide plant protection in the event of any of the analyzed accidents discussed in Reference 2, in which a loss of offsite power is assumed. LOVS channels are required to meet the redundancy and testability requirements of GDC 21 in 10 CFR 50, Appendix A (Ref. 5).

BASES

APPLICABLE SAFETY ANALYSES (continued)

The delay times assumed in the safety analysis for the ESF equipment include the [10] second DG start delay and the appropriate sequencing delay, if applicable. The response times for ESFAS actuated equipment in LCO 3.3.5, "Engineered Safety Features Actuation System (ESFAS) Instrumentation," include the appropriate DG loading and sequencing delay.

The DG - LOVS channels satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

The LCO for the LOVS requires that four channels per bus of each LOVS instrumentation Function be OPERABLE in MODES 1, 2, 3, and 4 and when the associated DG is required to be OPERABLE by LCO 3.8.2, "AC Sources - Shutdown." The LOVS supports safety systems associated with the ESFAS. In MODES 5 and 6, the four channels must be OPERABLE whenever the associated DG is required to be OPERABLE to ensure that the automatic start of the DG is available when needed.

Actions allow maintenance (trip channel) bypass of individual channels. Plants are restricted to 48 hours in a trip channel bypass condition before either restoring the Function to four channel operation (two-out-of-four logic) or placing the channel in trip (one-out-of-three logic). At units where adequate channel to channel independence has been demonstrated, specific exceptions have been approved by the NRC staff to permit one of the two-out-of-four channels to be bypassed for an extended period of time.

Loss of LOVS Function could result in the delay of safety system initiation when required. This could lead to unacceptable consequences during accidents. During the loss of offsite power, which is an anticipated operational occurrence, the DG powers the motor driven auxiliary feedwater pumps. Failure of these pumps to start would leave only the one turbine driven pump as well as an increased potential for a loss of decay heat removal through the secondary system.

Only Allowable Values are specified for each Function in the LCO. Nominal trip setpoints are specified in the plant specific setpoint calculations. The nominal setpoints are selected to ensure that the setpoint measured by CHANNEL FUNCTIONAL TESTS does not exceed the Allowable Value if the bistable is performing as required. Operation with a trip setpoint less conservative than the nominal trip setpoint, but within the Allowable Value, is acceptable, provided that operation and testing is consistent with the assumptions of the plant specific setpoint calculation. A channel is inoperable if its actual trip setpoint is not within its required Allowable Value.

BASES

APPLICABLE SAFETY ANALYSES (continued)

[For this unit, the Bases for the Allowable Values and trip setpoints are as follows:]

APPLICABILITY

The DG - LOVS actuation Function is required in MODES 1, 2, 3, and 4 because ESF Functions are designed to provide protection in these MODES. Actuation in MODE 5 or 6 is required whenever the required DG must be OPERABLE, so that it can perform its function on a loss of power or degraded power to the vital bus.

ACTIONS

A LOVS channel is inoperable when it does not satisfy the OPERABILITY criteria for the channel's function. The most common cause of channel inoperability is outright failure or drift of the bistable or process module sufficient to exceed the tolerance allowed by the plant specific setpoint analysis. Typically, the drift is found to be small and results in a delay of actuation rather than a total loss of function. Determination of setpoint drift is generally made during the performance of a CHANNEL FUNCTIONAL TEST when the instrument is set up for adjustment to bring it within specification. If the actual trip setpoint is not within the Allowable Value, the channel is inoperable and the appropriate Conditions must be entered.

In the event a channel's trip setpoint is found nonconservative with respect to the Allowable Value, or the channel is found inoperable, then all affected Functions provided by that channel must be declared inoperable and the LCO Condition entered. The required channels are specified on a per DG basis.

When the number of inoperable channels in a trip Function exceeds those specified in any related Condition associated with the same trip Function, then the plant is outside the safety analysis. Therefore, LCO 3.0.3 should be entered immediately if applicable in the current MODE of operation.

A Note has been added to clarify the application of Completion Time rules. The Conditions of this Specification may be entered independently for each DG - LOVS Function. The Completion Time(s) of the inoperable channel(s) of a Function will be tracked separately for each Function, starting from the time the Condition was entered for that Function.

A.1 and A.2

Condition A applies if one channel is inoperable for one or more Functions per DG bus.

BASES

ACTIONS (continued)

If the channel cannot be restored to OPERABLE status, the affected channel should either be bypassed or tripped within 1 hour (Required Action A.1).

Placing this channel in either Condition ensures that logic is in a known configuration. In trip, the LOVS Logic is one-out-of-three. In bypass, the LOVS Logic is two-out-of-three, and interlocks prevent bypass of a second channel for the affected Function. The 1 hour Completion Time is sufficient to perform these Required Actions.

Once Required Action A.1 has been complied with, Required Action A.2 allows prior to entering MODE 2 following the next MODE 5 entry to repair the inoperable channel. If the channel cannot be restored to OPERABLE status, the plant cannot enter MODE 2 following the next MODE 5 entry. The time allowed to repair or trip the channel is reasonable to repair the affected channel while ensuring that the risk involved in operating with the inoperable channel is acceptable. The prior to entering MODE 2 following the next MODE 5 entry Completion Time is based on adequate channel independence, which allows a two-out-of-three channel operation since no single failure will cause or prevent a reactor trip.

<u>B.1 and B.2</u>

Condition B applies if two channels are inoperable for one or more Functions.

If the channel cannot be placed in bypass or trip within 1 hour, the Conditions and Required Actions for the associated DG made inoperable by DG - LOVS instrumentation are required to be entered. Alternatively, one affected channel is required to be bypassed and the other is tripped, in accordance with Required Action B.2. This places the Function in one-out-of-two logic. The 1 hour Completion Time is sufficient to perform the Required Actions.

One of the two inoperable channels will need to be restored to OPERABLE status prior to the next required CHANNEL FUNCTIONAL TEST because channel surveillance testing on an OPERABLE channel requires that the OPERABLE channel be placed in bypass. However, it is not possible to bypass more than one DG - LOVS channel, and placing a second channel in trip will result in a loss of voltage diesel start signal. Therefore, if one DG - LOVS channel is in trip and a second channel is in bypass, a third inoperable channel would place the unit in LCO 3.0.3.

BASES

ACTIONS (continued)

After one channel is restored to OPERABLE status, the provisions of Condition A still apply to the remaining inoperable channel.

C.1

Condition C applies when more than two undervoltage or Degraded Voltage channels on a single bus are inoperable.

Required Action C.1 requires all but two channels to be restored to OPERABLE status within 1 hour. With more than two channels inoperable, the logic is not capable of providing the DG - LOVS signal for valid Loss of Voltage or Degraded Voltage conditions. The 1 hour Completion Time is reasonable to evaluate and take action to correct the degraded condition in an orderly manner and takes into account the low probability of an event requiring LOVS occurring during this interval.

D.1

Condition D applies if the Required Actions and associated Completion Times are not met.

Required Action D.1 ensures that Required Actions for the affected DG inoperabilities are initiated. Depending upon plant MODE, the ACTIONS specified in LCO 3.8.1, "AC Sources - Operating," or LCO 3.8.2 are required immediately.

SURVEILLANCE REQUIREMENTS

The following SRs apply to each DG - LOVS Function.

[SR 3.3.7.1

Performance of the CHANNEL CHECK once every 12 hours ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the indicated output of the potential transformers that feed the LOVS undervoltage relays. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value. Significant deviations between the two channels could be an indication of excessive drift in one of the channels or of something even more serious. CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying that the instrumentation continues to operate properly between each CHANNEL CALIBRATION.]

BASES

SURVEILLANCE REQUIREMENTS (continued)

[Agreement criteria are determined by the plant staff based on a combination of channel instrument uncertainties, including indication and readability. If the channels are within the criteria, it is an indication that the channels are OPERABLE.

The Frequency, about once every shift, is based upon operating experience that demonstrates channel failure is rare. Since the probability of two random failures in redundant channels in any 12 hour period is extremely low, the CHANNEL CHECK minimizes the chance of loss of protective function due to failure of redundant channels. The CHANNEL CHECK supplements less formal, but more frequent, checks of channel OPERABILITY during normal operational use of the displays associated with the LCO required channels.]

SR 3.3.7.2

A CHANNEL FUNCTIONAL TEST is performed every [92] days to ensure that the entire channel will perform its intended function when needed. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

The Frequency of [92] days is based on plant operating experience with regard to channel OPERABILITY and drift, which demonstrates that failure of more than one channel of a given Function in any [92] day Frequency is a rare event. Any setpoint adjustment shall be consistent with the assumptions of the current plant specific setpoint analysis.

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the surveillance interval extension analysis. The requirements for this review are outlined in Reference [6].

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.7.3

SR 3.3.7.3 is the performance of a CHANNEL CALIBRATION every [18] months. The CHANNEL CALIBRATION verifies the accuracy of each component within the instrument channel. This includes calibration of the undervoltage relays and demonstrates that the equipment falls within the specified operating characteristics defined by the manufacturer. The Surveillance verifies that the channel responds to a measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drift between successive surveillances to ensure the instrument channel remains operational. CHANNEL CALIBRATIONS must be performed consistent with the plant specific setpoint analysis. Any setpoint adjustment shall be consistent with the assumptions of the current plant specific setpoint analysis.

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the surveillance interval extension analysis. The requirements for this review are outlined in Reference [6].

The setpoints, as well as the response to a Loss of Voltage and Degraded Voltage test, shall include a single point verification that the trip occurs within the required delay time, as shown in Reference 1. The Frequency is based upon the assumption of an [18] month calibration interval for the determination of the magnitude of equipment drift in the setpoint analysis.

REFERENCES

1. FSAR, Section [8.3].

2. FSAR, Chapter [15].

3. "Plant Protection System Selection of Trip Setpoint Values."

4. IEEE Standard 279-1971.

5. 10 CFR 50, Appendix A, GDC 21.

6. [ ].

B 3.3 INSTRUMENTATION

B 3.3.8 Containment Purge Isolation Signal (CPIS) (Digital)

BASES

BACKGROUND

This LCO encompasses the CPIS, which is a plant specific instrumentation channel that performs an actuation function required for plant protection but is not otherwise included in LCO 3.3.6, "Engineered Safety Features Actuation System (ESFAS) Logic and Manual Trip," or LCO 3.3.7, "Diesel Generator (DG) - Loss of Voltage Start (LOVS)." Individual plants shall include the CPIS Function and LCO requirements that are applicable to them.

The CPIS provides protection from the release of radioactive contamination from the containment in the event a fuel assembly should be severely damaged during handling. It also closes the purge valves during plant operation in response to a Reactor Coolant System (RCS) leak.

The CPIS will detect any abnormal amounts of radioactive material in the containment and will initiate purge valve closure to limit the release of radioactivity to the environment. Both the minipurge and large volume purge supply and exhaust valves are closed on a CPIS when a high radiation level in containment is detected.

The CPIS includes two independent, redundant logic subsystems, including actuation trains. Each train employs four sensors, each one detecting one of the following:

- Gaseous
- Airborne particulate
- Iodine
- Gamma (area)

If any one of these sensors exceeds the bistable trip setpoint, the CPIS train will be actuated (one-out-of-four logic).

Each train actuates a separate series valve in the containment purge supply and return lines. Either train controls sufficient equipment to perform the isolation function. These valves are also isolated on a Safety Injection Actuation Signal (SIAS) and Containment Isolation Actuation Signal (CIAS).

BASES

BACKGROUND (continued)

Trip Setpoints and Allowable Values

Trip setpoints used in the bistables are based on the analytical limits (Ref. 1). The selection of these trip setpoints is such that adequate protection is provided when all sensor and processing time delays are taken into account. To allow for calibration tolerances, instrumentation uncertainties, and instrument drift, trip setpoint Allowable Values specified in LCO 3.3.8 are conservatively adjusted with respect to the analytical limits. A detailed description of the methodology used to calculate the trip setpoints, including their explicit uncertainties, is provided in "Plant Protection System Selection of Trip Setpoint Values" (Ref. 2). The actual nominal trip setpoint entered into the bistable is normally still more conservative than that specified by the Allowable Value to account for changes in random measurement errors detectable by a CHANNEL FUNCTIONAL TEST. One example of such a change in measurement error is drift during the surveillance interval. If the measured setpoint does not exceed the Allowable Value, the bistable is considered OPERABLE.

Setpoints in accordance with the Allowable Value will ensure that safety limits are not violated during anticipated operational occurrences (AOOs) and the consequences of Design Basis Accidents will be acceptable, providing the plant is operated from within the LCOs at the onset of the AOO or accident and the equipment functions as designed.

APPLICABLE SAFETY ANALYSES

The CPIS is a backup to the CIAS systems in MODES 1, 2, 3, and 4 and will close the containment purge valves in the event of high radiation levels resulting from a primary leak in the containment.

The CPIS is also required to close the containment purge valves in the event of the fuel handling accident in containment [involving handling recently irradiated fuel (i.e., fuel that has occupied part of a critical reactor core within the previous [X] days)], as described in Reference 1. This accident is a limiting case representing a class of accidents that might involve radiation release in containment without CIAS actuation. The CPIS ensures the consequences of a dropped [recently] irradiated fuel assembly in containment are not as severe as a dropped [recently] irradiated assembly in the fuel handling building. This ensures that the offsite consequences of radiation accidents in containment are within 10 CFR 100 limits (Ref. 3).

The CPIS satisfies the requirements of Criterion 3 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO

LCO 3.3.8 requires one CPIS channel to be OPERABLE. The required channel consists of [particulate, iodine, gaseous, and area radiation monitors]; Actuation Logic; and Manual Trip. The specific Allowable Values for the setpoints of the CPIS are listed in the SRs.

Only the Allowable Values are specified for each trip Function in the LCO. Operation with a trip setpoint less conservative than the nominal trip setpoint, but within its Allowable Value, is acceptable, provided that the difference between the nominal trip setpoint and the Allowable Value is equal to or greater than the drift allowance assumed for each trip in the transient and accident analyses. A channel is inoperable if its actual trip setpoint is not within its Allowable Value.

Each Allowable Value specified is more conservative than the analytical limit assumed in the transient and accident analysis in order to account for instrument uncertainties appropriate to the trip function. These uncertainties are defined in the "Plant Protection System Selection of Trip Setpoint Values" (Ref. 2).

The Bases for the LCO on CPIS are discussed below for each Function:

a. Manual Trip

The LCO on Manual Trip backs up the automatic trip and ensures operators have the capability to rapidly initiate the CPIS Function if any parameter is trending toward its setpoint. Only one manual channel of CPIS is required in MODES 1, 2, 3, and 4, since the CPIS is redundant with the CIAS and SIAS. Only one manual channel of CPIS is required during CORE ALTERATIONS and movement of irradiated fuel assemblies, since there are additional means of closing the containment purge valves in the event of a channel failure.

b. Airborne Radiation and Containment Area Radiation

The LCO on the radiation channels requires that each channel be OPERABLE for each Actuation Logic channel, since they are not totally redundant to each other.

The trip setpoint of twice background is selected to allow detection of small deviations from normal. The absolute value of the trip setpoint in MODES 5 and 6 differs from the setpoint in MODES 1, 2, 3, and 4 so that a fuel handling accident can be detected in the lower background radiation expected in these MODES.

BASES

LCO (continued)

c. Actuation Logic

One channel of Actuation Logic is required, since the valves can be shut independently of the CPIS signal either manually from the control room or using either the SIAS or CIAS push button.

APPLICABILITY

In MODES 1, 2, 3, and 4, the minipurge valves may be open. In the MODES, it is necessary to ensure the valves will shut in the event of a primary leak in containment whenever any of the containment purge valves are open.

With the purge valves open during movement of [recently] irradiated fuel assemblies within containment, there is the possibility of a fuel handling accident requiring CPIS on high radiation in containment. [Due to radioactive decay, CPIS is only required to mitigate fuel handling accidents involving handling recently irradiated fuel (i.e., fuel that has occupied part of a critical reactor core within the previous [X] days).]

The APPLICABILITY is modified by a Note, which states that the CPIS Specification is only required when the penetration is not isolated by at least one closed and de-activated automatic valve, closed manual valve, or blind flange.

ACTIONS

A CPIS channel is inoperable when it does not satisfy the OPERABILITY criteria for the channel's function. The most common cause of channel inoperability is outright failure or drift of the bistable or process module sufficient to exceed the tolerance allowed by the plant specific setpoint analysis. Typically, the drift is not large and would result in a delay of actuation rather than a total loss of function. This determination is generally made during the performance of a CHANNEL FUNCTIONAL TEST when the process instrument is set up for adjustment to bring it within specification. If the trip setpoint is not consistent with the Allowable Value, the channel must be declared inoperable immediately, and the appropriate Conditions must be entered.

In the event a channel's trip setpoint is found nonconservative with respect to the Allowable Value, or the sensor, instrument loop, signal processing electronics, or bistable is found inoperable, then all affected Functions provided by that channel are required to be declared inoperable and the LCO Condition entered for the particular protective function affected.

BASES

ACTIONS (continued)

When the number of inoperable channels in a trip Function exceeds that specified in any related Condition associated with the same trip Function, then the plant is outside the safety analysis. Therefore, LCO 3.0.3 is immediately entered if applicable in the current MODE of operation.

A.1

Condition A applies to the failure of CPIS Manual Trip, Actuation Logic, and required [particulate, iodine, gaseous, and area radiation monitors]. The Required Action is to enter the applicable Conditions and Required Actions for affected valves of LCO 3.6.3, "Containment Isolation Valves." The Completion Time accounts for the condition that the capability to isolate containment on valid containment high radiation or manual signals is degraded during power operation or shutdown modes.

B.1 and B.2

Condition B applies when the Required Action and associated Completion Time of Condition A are not met in MODE 1, 2, 3, or 4. If Required Action A cannot be met within the required Completion Time, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 5 within 36 hours.

C.1 and C.2

Condition C applies to the same conditions as are described in Condition A; however, the applicability is during the movement of [recently] irradiated fuel assemblies within containment. Required Action C.1 is to place the containment purge and exhaust isolation valves in the closed position. The Required Action immediately performs the isolation function of the CPIS. Required Action C.2 may be performed in lieu of Required Action C.1. Required Action C.2 requires suspension of movement of [recently] irradiated fuel in containment immediately. The Completion Time accounts for the fact that the automatic capability to isolate containment on valid containment high radiation signals is degraded during conditions in which a fuel handling accident is possible and CPIS provides the only required automatic mitigation of radiation release.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.3.8.1

Performance of the CHANNEL CHECK once every 12 hours ensures that a gross failure of instrumentation has not occurred on the required area and gaseous radiation monitor channels used in the CPIS. A CHANNEL CHECK is normally a comparison of the parameter indicated on one channel to a similar parameter on other channels. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value.

Significant deviations between the two instrument channels could be an indication of excessive instrument drift in one of the channels or of something even more serious. CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

Agreement criteria are determined by the plant staff based on a combination of the channel instrument uncertainties, including indication and readability. If a channel is outside the criteria, it may be an indication that the transmitter or the signal processing equipment has drifted outside its limit.

The Frequency, about once every shift, is based on operating experience that demonstrates the rarity of channel failure. Since the probability of two random failures in redundant channels in any 12 hour period is low, the CHANNEL CHECK minimizes the chance of loss of protective function due to failure of redundant channels. The CHANNEL CHECK supplements less formal, but more frequent, checks of channel OPERABILITY during normal operational use of the displays associated with the LCO required channels.

SR 3.3.8.2

SR 3.3.8.2 is the performance of a CHANNEL CHECK on the particulate and iodine channels used in the CPIS. It differs only in the Frequency, which is weekly. These channels use a filter to trap the particulate and iodine activity prior to the air sample being pumped to the gaseous activity chamber. This technique results in an integration of total particulate and iodine activity until the filter assemblies are replaced. The low levels of activity expected make more frequent monitoring unnecessary.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.8.3

A CHANNEL FUNCTIONAL TEST is performed on the required containment radiation monitoring channel to ensure the entire channel will perform its intended function. Setpoints must be found within the Allowable Values specified in SR 3.3.8.3 and left consistent with the assumptions of the plant specific setpoint analysis (Ref. 4). A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions. The Frequency of 92 days is based on plant operating experience with regard to channel OPERABILITY and drift, which demonstrates that failure of more than one channel of a given Function in any 92 day Frequency is a rare event.

A Note to the SR indicates this Surveillance is required to be met in MODES 1, 2, 3, and 4 only.

SR 3.3.8.4

A CHANNEL FUNCTIONAL TEST is performed on the required containment radiation monitoring channel to ensure the entire channel will perform its intended function. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions. Setpoints must be found within the Allowable Values specified in SR 3.3.8.4 and left consistent with the assumptions of the plant specific setpoint methodology (Ref. 4). The Frequency of 92 days is based on plant operating experience with regard to channel OPERABILITY and drift, which demonstrates that failure of more than one channel of a given Function in any 92 day interval is a rare event.

A Note to the SR indicates that this test is only required to be met during CORE ALTERATIONS or during movement of irradiated fuel assemblies within containment.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.8.5

Proper operation of the individual initiation relays is verified by actuating these relays during the CHANNEL FUNCTIONAL TEST of the Actuation Logic every [18] months. This will actuate the Function, operating all associated equipment. Proper operation of the equipment actuated by each train is thus verified. The Frequency of [18] months is based on plant operating experience with regard to channel OPERABILITY and drift, which demonstrates that failure of more than one channel of a given Function during any [18] month interval is a rare event. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions. A Note to the SR indicates that this Surveillance includes verification of operation for each initiation relay.

SR 3.3.8.6

CHANNEL CALIBRATION is a complete check of the instrument channel including the sensor. The Surveillance verifies that the channel responds to a measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drift between successive calibrations to ensure that the channel remains operational between successive surveillances. CHANNEL CALIBRATIONS must be performed consistent with the plant specific setpoint analysis.

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the surveillance interval extension analysis. The requirements for this review are outlined in Reference [5].

The [18] month Frequency is based on the need to perform this Surveillance under the conditions that apply during a plant outage and the potential for an unplanned transient if the Surveillance were performed with the reactor at power.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.8.7

This Surveillance ensures that the train actuation response times are less than or equal to the maximum times assumed in the analyses. The [18] month Frequency is based upon plant operating experience, which shows that random failures of instrumentation components causing serious response time degradation, but not channel failure, are infrequent occurrences. Testing of the final actuating devices, which make up the bulk of the response time, is included in the Surveillance.

SR 3.3.8.8

Every [18] months, a CHANNEL FUNCTIONAL TEST is performed on the CPIS Manual Trip channel. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

This test verifies that the trip push buttons are capable of opening contacts in the Actuation Logic as designed, de-energizing the initiation relays and providing manual actuation of the Function. The [18] month Frequency is based on the need to perform this Surveillance under the conditions that apply during a plant outage and the potential for an unplanned transient if the Surveillance were performed with the reactor at power. Operating experience has shown these components usually pass the Surveillance when performed at a Frequency of once every [18] months.

REFERENCES

1. FSAR, Chapter [15].

2. "Plant Protection System Selection of Trip Setpoint Values."

3. 10 CFR 100.

4. Plant Specific Setpoint Methodology.

5. [ ].

B 3.3 INSTRUMENTATION

B 3.3.9 Control Room Isolation Signal (CRIS) (Digital)

BASES

BACKGROUND

This LCO encompasses CRIS actuation, which is a plant specific instrumentation channel that performs an actuation Function required for plant protection but is not otherwise included in LCO 3.3.6, "Engineered Safety Features Actuation System (ESFAS) Logic and Manual Trip," or LCO 3.3.7, "Diesel Generator (DG) - Loss of Voltage Start (LOVS)." This is a non-Nuclear Steam Supply System ESFAS Function that, because of differences in purpose, design, and operating requirements, is not included in LCO 3.3.6 and LCO 3.3.7. Details of this LCO are for illustration only. Individual plants shall include those Functions and LCO requirements that are applicable to them.

The CRIS terminates the normal supply of outside air to the control room and initiates actuation of the Emergency Radiation Protection System to minimize operator radiation exposure. The CRIS includes two independent, redundant subsystems, including actuation trains. Each train employs two separate sensors. One sensor detects gaseous activity. The other detects particulate and iodine activity. Since the two sensors detect different types of activity, they are not considered redundant to each other. However, since there are separate sensors in each train, the trains are redundant. If the bistable monitoring either sensor indicates an unsafe condition, that train will be actuated (one-out-of-two logic). The two trains actuate separate equipment. Actuating either train will perform the intended function. Control room isolation also occurs on a Safety Injection Actuation Signal (SIAS).

<u>Trip Setpoints and Allowable Values</u>

Trip setpoints used in the bistables are based on the analytical limits (Ref. 1). The selection of these trip setpoints is such that adequate protection is provided when all sensor and processing time delays are taken into account. To allow for calibration tolerances, instrumentation uncertainties, and instrument drift, Allowable Values specified in LCO 3.3.9 are conservatively adjusted with respect to the analytical limits. A detailed description of the methodology used to calculate the trip setpoints, including their explicit uncertainties, is provided in "Plant Protection System Selection of Trip Setpoint Values" (Ref. 2). The actual nominal trip setpoint entered into the bistable is normally still more

BASES

BACKGROUND (continued)

conservative than that specified by the Allowable Value to account for changes in random measurement errors detectable by a CHANNEL FUNCTIONAL TEST. One example of such a change in measurement error is drift during the surveillance interval. If the measured setpoint does not exceed the Allowable Value, the bistable is considered OPERABLE.

Setpoints in accordance with the Allowable Value will ensure that Safety Limits are not violated during anticipated operational occurrences (AOOs) and the consequences of Design Basis Accidents will be acceptable, providing the plant is operated from within the LCOs at the onset of the AOO or accident and the equipment functions as designed.

APPLICABLE SAFETY ANALYSES

The CRIS, in conjunction with the Control Room Emergency Air Cleanup System (CREACS), maintains the control room atmosphere within conditions suitable for prolonged occupancy throughout the duration of any one of the accidents discussed in Reference 1. The radiation exposure of control room personnel, through the duration of any one of the postulated accidents discussed in "Accident Analysis," FSAR, Chapter [15] (Ref. 1), does not exceed the limits set by 10 CFR 50, Appendix A, GDC 19 (Ref. 3).

The CRIS satisfies the requirements of Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

LCO 3.3.9 requires one channel of CRIS to be OPERABLE. The required channel consists of Actuation Logic, Manual Trip, and [particulate/iodine and gaseous radiation monitors]. The specific Allowable Values for the setpoints of the CRIS are listed in the SRs.

Only the Allowable Values are specified for each trip Function in the LCO. Operation with a trip setpoint less conservative than the nominal trip setpoint, but within its Allowable Value, is acceptable, provided that the difference between the nominal trip setpoint and the Allowable Value is equal to or greater than the drift allowance assumed for each trip in the transient and accident analyses.

Each Allowable Value specified is more conservative than the analytical limit assumed in the transient and accident analysis in order to account for instrument uncertainties appropriate to the trip Function. These uncertainties are defined in the "Plant Protection System Selection of Trip Setpoint Values" (Ref. 2). A channel is inoperable if its actual trip setpoint is not within its required Allowable Value.

BASES

APPLICABLE SAFETY ANALYSES (continued)

The Bases for the LCO on the CRIS are discussed below for each Function:

a. Manual Trip

The LCO on Manual Trip backs up the automatic trips and ensures operators have the capability to rapidly initiate the CRIS Function if any parameter is trending toward its setpoint. One channel must be OPERABLE. This considers that the Manual Trip capability is a backup and that other means are available to actuate the redundant train if required, including manual SIAS.

b. Airborne Radiation

Both channels of Airborne Radiation detection in the required train are required to be OPERABLE to ensure the control room isolates on either high iodine and high particulate or gaseous concentration.

[For this unit, the basis for the Allowable Value is as follows:]

c. Actuation Logic

One train of Actuation Logic must be OPERABLE, since there are alternate means available to actuate the redundant train, including SIAS.

APPLICABILITY

The CRIS Functions must be OPERABLE in MODES 1, 2, 3, 4, [5, and 6] and during movement of [recently] irradiated fuel assemblies to ensure a habitable environment for the control room operators. [Due to radioactive decay, CRIS is only required to mitigate fuel handling accidents involving handling recently irradiated fuel (i.e., fuel that has occupied part of a critical reactor core within the previous [X] days)].

----------------------------------REVIEWER'S NOTE----------------------------------
For those plants that credit gas decay tank rupture accidents, the CRIS must also be OPERABLE in MODES 5 and 6.

ACTIONS

A CRIS channel is inoperable when it does not satisfy the OPERABILITY criteria for the channel's function. The most common cause of channel inoperability is outright failure or drift of the bistable or process module sufficient to exceed the tolerance allowed by the plant specific setpoint analysis. Typically, the drift is not large and would result in a delay of actuation rather than a total loss of function. This determination is

BASES

ACTIONS (continued)

generally made during the performance of a CHANNEL FUNCTIONAL TEST when the process instrument is set up for adjustment to bring it within specification. If the trip setpoint is not within the Allowable Value, the channel is inoperable and the appropriate Conditions must be entered.

A.1, B.1, B.2, C.1, C.2.1, and C.2.2

Conditions A and C have been modified by a Note, which specifies that CREACS be placed manually in the toxic gas protection mode if the automatic transfer to the toxic gas protection mode is inoperable. [At this unit, the basis for this Note is as follows:]

Conditions A, B, and C are applicable to manual and automatic actuation of the CREACS by CRIS. Condition A applies to the failure of the CRIS Manual Trip, Actuation Logic, and required [particulate/iodine and required gaseous radiation monitor channels] in MODE 1, 2, 3, or 4. Entry into this Condition requires action to either restore the failed channel(s) or manually perform the CRIS safety function (Required Action A.1). The Completion Time of 1 hour is sufficient to complete the Required Actions and accounts for the fact that CRIS supplements control room isolation by other Functions (e.g., SIAS) in MODES 1, 2, 3, and 4. If the channel cannot be restored to OPERABLE status, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours (Required Action B.1) and to MODE 5 within 36 hours (Required Action B.2). The Completion Times of 6 hours and 36 hours for reaching MODES 3 and 5 from MODE 1 are reasonable, based on operating experience and normal cooldown rates, for reaching the required MODE from full power conditions in an orderly manner and without challenging plant safety systems or operators.

Condition C applies to the failure of CRIS Manual Trip, Actuation Logic, and required particulate/iodine and required gaseous radiation monitor channels [in MODE 5 or 6] or when moving [recently] irradiated assemblies. The Required Actions are immediately taken to place one OPERABLE CREACS train in the emergency radiation protection mode, or to suspend positive reactivity additions and movement of [recently] irradiated fuel assemblies. The Completion Time recognizes the fact that the radiation signals are the only Functions available to initiate control room isolation in the event of a fuel handling accident [involving handling recently irradiated fuel].

BASES

ACTIONS (continued)

Required Action [C.2.2 is modified by a Note to indicate that normal plant control operations that individually add limited positive reactivity (e.g., temperature or boron fluctuations associated with RCS inventory management or temperature control) are not precluded by this Action, provided they are accounted for in the calculated SDM.

SURVEILLANCE REQUIREMENTS

SR 3.3.9.1

Performance of the CHANNEL CHECK once every 12 hours ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the parameter indicated on one channel to a similar parameter on other channels. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value.

Significant deviations between the two instrument channels could be an indication of excessive instrument drift in one of the channels or of something even more serious. CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

Agreement criteria are determined by the plant staff based on a combination of the channel instrument uncertainties, including indication and readability. If a channel is outside the criteria, it may be an indication that the transmitter or the signal processing equipment has drifted outside its limit.

The Frequency, about once every shift, is based on operating experience that demonstrates the rarity of channel failure. Since the probability of two random failures in redundant channels in any 12 hour period is low, the CHANNEL CHECK minimizes the chance of loss of protective function due to failure of redundant channels. The CHANNEL CHECK supplements less formal, but more frequent, checks of channel OPERABILITY during normal operational use of the displays associated with the LCO required channels.

At this unit, the following administrative controls and design features (e.g., downscale alarms) immediately alert operations to loss of function in the nonredundant channels.

[At this unit, verification of sample system alignment and operation for gaseous, particulate, and iodine monitors is required as follows:]

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.9.2

A CHANNEL FUNCTIONAL TEST is performed on the required control room radiation monitoring channel to ensure the entire channel will perform its intended function. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions. Any setpoint adjustment shall be consistent with the assumptions of the current plant specific setpoint analysis.

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the frequency extension analysis. The requirements for this review are outlined in Reference [4].

The Frequency of [92] days is based on plant operating experience with regard to channel OPERABILITY and drift, which demonstrates that failure of more than one channel of a given Function in any [92] day interval is a rare event.

SR 3.3.9.3

Proper operation of the individual initiation relays is verified by de-energizing these relays during the CHANNEL FUNCTIONAL TEST of the Actuation Logic every [18] months. This will actuate the Function, operating all associated equipment. Proper operation of the equipment actuated by each train is thus verified. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

The Frequency of [18] months is based on plant operating experience with regard to channel OPERABILITY, which demonstrates that failure of more than one channel of a given Function in any [18] month interval is a rare event.

BASES

SURVEILLANCE REQUIREMENTS (continued)

Note 1 indicates this Surveillance includes verification of operation for each initiation relay.

Note 2 indicates that relays that cannot be tested at power are excepted from the Surveillance Requirement while at power. These relays must, however, be tested during each entry into MODE 5 exceeding 24 hours unless they have been tested within the previous 6 months.

SR 3.3.9.4

CHANNEL CALIBRATION is a complete check of the instrument channel including the sensor. The Surveillance verifies that the channel responds to a measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drift between successive calibrations to ensure that the channel remains operational between successive surveillances. CHANNEL CALIBRATIONS must be performed consistent with the plant specific setpoint analysis.

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the surveillance interval extension analysis. The requirements for this review are outlined in Reference [4].

The Frequency is based upon the assumption of an [18] month calibration interval for the determination of the magnitude of equipment drift in the setpoint analysis.

SR 3.3.9.5

Every [18] months, a CHANNEL FUNCTIONAL TEST is performed on the manual CRIS actuation circuitry. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

BASES

SURVEILLANCE REQUIREMENTS (continued)

This test verifies that the trip push buttons are capable of opening contacts in the Actuation Logic as designed, de-energizing the initiation relays and providing Manual Trip of the function. The [18] month Frequency is based on the need to perform this Surveillance under the conditions that apply during a plant outage and the potential for an unplanned transient if the Surveillance were performed with the reactor at power. Operating experience has shown these components usually pass the Surveillance when performed at a Frequency of once every [18] months.

[SR 3.3.9.6

This Surveillance ensures that the train actuation response times are less than the maximum times assumed in the analyses. The [18] month Frequency is based upon plant operating experience, which shows that random failures of instrumentation components causing serious response time degradation, but not channel failure, are infrequent occurrences. Testing of the final actuating devices, which make up the bulk of the response time, is included in the Surveillance testing.]

REFERENCES

1. FSAR, Chapter [15].
2. "Plant Protection System Selection of Trip Setpoint Values."
3. 10 CFR 50, Appendix A, GDC 19.
4. [ ].

B 3.3 INSTRUMENTATION

B 3.3.10 Fuel Handling Isolation Signal (FHIS) (Digital)

BASES

BACKGROUND

This LCO encompasses FHIS actuation, which is a plant specific instrumentation channel that performs an actuation Function required for plant protection but is not otherwise included in LCO 3.3.6, "Engineered Safety Features Actuation System (ESFAS) Logic and Manual Trip," or LCO 3.3.7, "Diesel Generator (DG) - Loss of Voltage Start (LOVS)." This is a non-Nuclear Steam Supply System ESFAS Function that, because of differences in purpose, design, and operating requirements, is not included in LCO 3.3.6 and LCO 3.3.7. Details of this LCO are for illustration only. Individual plants shall include those Functions and LCO requirements that are applicable to them.

The FHIS provides protection from radioactive contamination in the spent fuel pool area in the event that a spent fuel element ruptures during handling.

The FHIS will detect radioactivity from fission products in the fuel and will initiate appropriate actions so the release to the environment is limited. More detail is provided in Reference 1.

The FHIS includes two independent, redundant subsystems, including actuation trains. Each train employs two separate sensors. One sensor detects gaseous activity. The other detects particulate and iodine activity. Since the two sensors detect different types of activity, they are not considered redundant to each other. However, since there are separate sensors in each train, the trains are redundant. If the bistable monitoring either sensor indicates an unsafe condition, that train will be actuated (one-out-of-two logic). The two trains actuate separate equipment.

Trip Setpoints and Allowable Values

Trip setpoints used in the bistables are based on the analytical limits (Ref. 2). The selection of these trip setpoints is such that adequate protection is provided when all sensor and processing time delays are taken into account. To allow for calibration tolerances, instrumentation uncertainties, and instrument drift, Allowable Values specified in LCO 3.3.10 are conservatively adjusted with respect to the analytical limits. A detailed description of the methodology used to calculate the trip setpoints, including their explicit uncertainties, is provided in "Plant

BASES

BACKGROUND (continued)

Protection System Selection of Trip Setpoint Values" (Ref. 3). The actual nominal trip setpoint entered into the bistable is normally still more conservative than that specified by the Allowable Value to account for changes in random measurement errors detectable by a CHANNEL FUNCTIONAL TEST. One example of such a change in measurement error is drift during the surveillance interval. If the measured setpoint does not exceed the Allowable Value, the bistable is considered OPERABLE.

Setpoints in accordance with the Allowable Value will ensure that Safety Limits are not violated during anticipated operational occurrences (AOOs) and the consequences of Design Basis Accidents will be acceptable, providing the plant is operated from within the LCOs at the onset of the AOO or accident and the equipment functions as designed.

APPLICABLE SAFETY ANALYSES

The FHIS is required to isolate the normal Fuel Building Air Cleanup System (FBACS) and automatically initiate the recirculation and filtration systems in the event of the fuel handling accident [involving handling recently irradiated fuel] in the fuel handling building, as described in Reference 2. The FHIS helps ensure acceptable consequences for the dropping of a spent fuel bundle breaching up to 60 fuel pins.

The FHIS satisfies the requirements of Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

LCO 3.3.10 requires one channel of FHIS to be OPERABLE. The required channel consists of Actuation Logic, Manual Trip, and [particulate/iodine and] gaseous radiation monitors. The specific Allowable Values for the setpoints of the FHIS are listed in the SRs.

Only the Allowable Values are specified for each trip Function in the SRs. Operation with a trip setpoint less conservative than the nominal trip setpoint, but within its Allowable Value, is acceptable, provided that the difference between the nominal trip setpoint and the Allowable Value is equal to or greater than the drift allowance assumed for each trip in the transient and accident analyses.

Each Allowable Value specified is more conservative than the analytical limit assumed in the transient and accident analysis in order to account for instrument uncertainties appropriate to the trip Function. These uncertainties are defined in the "Plant Protection System Selection of Trip Setpoint Values" (Ref. 3).

BASES

LCO (continued)

The Bases for the LCO on the FHIS are discussed below for each Function:

a. Manual Trip

The LCO on Manual Trip ensures that the FHIS Function can easily be initiated if any parameter is trending rapidly toward its setpoint. Components can be actuated independently of the FHIS. Both available channels are required to ensure a single failure will not disable automatic initiation capability.

b. Airborne Radiation

The LCO on the two Airborne Radiation channels requires that each channel be OPERABLE for the required Actuation Logic channel, since they are not redundant to each other.

[At this plant, the basis for the FHIS radiation monitor Allowable Values is as follows:]

c. Actuation Logic

Two channels of Actuation Logic are required to be OPERABLE to ensure no single random failure can prevent automatic actuation.

APPLICABILITY

One FHIS channel is required to be OPERABLE during movement of [recently] irradiated fuel in the fuel building. The FHIS isolates the fuel building area in the event of a fuel handling accident [involving handling recently irradiated fuel].

[The FHIS is required to be OPERABLE in MODES 1, 2, 3, and 4 and during movement of [recently] irradiated fuel because the fuel building heating, ventilation, and air conditioning (HVAC) is shared with Engineered Safety Features (ESF) equipment.]

The FHIS must be OPERABLE in [MODES 1, 2, 3, and 4] and during movement of [recently] irradiated fuel in the fuel building, since the FHIS isolates the fuel handling area in the event of a fuel handling accident in any MODE or other condition. [Due to radioactive decay, FHIS is only required to mitigate fuel handling accidents involving handling recently irradiated fuel (i.e., fuel that has occupied part of a critical reactor core within the previous [X] days).]

BASES

ACTIONS

LCO 3.0.3 is not applicable while in MODE 5 or 6. However, since irradiated fuel assembly movement can occur in MODE 1, 2, 3, or 4, the ACTIONS have been modified by a Note stating that LCO 3.0.3 is not applicable. If moving irradiated fuel assemblies while in MODE 5 or 6, LCO 3.0.3 would not specify any action. If moving irradiated fuel assemblies while in MODE 1, 2, 3, or 4, the fuel movement is independent of reactor operations. Entering LCO 3.0.3, while in MODE 1, 2, 3, or 4 would require the unit to be shutdown unnecessarily.

An FHIS channel is inoperable when it does not satisfy the OPERABILITY criteria for the channel's function. The most common cause of channel inoperability is outright failure or drift of the bistable or process module sufficient to exceed the tolerance allowed by the plant specific setpoint analysis. Typically, the drift is not large and would result in a delay of actuation rather than a total loss of function. This determination is generally made during the performance of a CHANNEL FUNCTIONAL TEST when the process instrument is set up for adjustment to bring it within specification. If the trip setpoint is not consistent with the Allowable Value in LCO 3.3.10, the channel must be declared inoperable immediately and the appropriate Conditions must be entered.

In the event a channel's trip setpoint is found nonconservative with respect to the Allowable Value, or the sensor, instrument loop, signal processing electronics, or bistable is found inoperable, then all affected Functions provided by that channel are required to be declared inoperable and the LCO Condition entered for the particular protective function affected.

When the number of inoperable channels in a trip Function exceeds that specified in any related Condition associated with the same trip Function, then the plant is outside the safety analysis. Therefore, LCO 3.0.3 is immediately entered if applicable in the current MODE of operation.

[<u>A.1, B.1, and B.2</u>

Conditions A and B apply only to those plants whose fuel building HVAC is shared with an ESF equipment room.

Condition A applies to FHIS Manual Trip, Actuation Logic, and required [particulate/iodine and gaseous radiation monitors] inoperable.

BASES

ACTIONS (continued)

The Required Actions are to restore the affected channels to OPERABLE status or place one OPERABLE FBACS train in operation within 1 hour. The Completion Time of 1 hour is sufficient to perform the Required Actions. The Completion Time accounts for the fact that the FHIS radiation monitors are the only signals available to automatically initiate the FBACS to mitigate radiation releases in the fuel building and credits the relatively lower likelihood of such events when irradiated fuel is not being moved.

Condition B applies if the affected channels cannot be restored to OPERABLE status or one OPERABLE FBACS train cannot be placed in operation. If the channels cannot be restored to OPERABLE status, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 5 within 36 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required MODE from full power conditions in an orderly manner and without challenging plant systems.]

<u>C.1 and C.2</u>

Condition C applies to FHIS Manual Trip, Actuation Logic, and required [particulate/iodine and] gaseous radiation monitor inoperable during movement of [recently] irradiated fuel in the fuel building.

The Required Actions are to restore required channels to OPERABLE status, or place one OPERABLE FBACS train in operation, or suspend movement of [recently] irradiated fuel in the fuel building. These Required Actions are required to be completed immediately. The Completion Time accounts for the higher likelihood of releases in the fuel building during fuel handling.

SURVEILLANCE REQUIREMENTS

<u>SR 3.3.10.1</u>

Performance of the CHANNEL CHECK once every 12 hours ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the parameter indicated on one channel to a similar parameter on other channels. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value.

BASES

SURVEILLANCE REQUIREMENTS (continued)

Significant deviations between the two instrument channels could be an indication of excessive instrument drift in one of the channels or of something even more serious. CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

Agreement criteria are determined by the plant staff based on a combination of the channel instrument uncertainties, including indication and readability. If a channel is outside the criteria, it may be an indication that the transmitter or the signal processing equipment has drifted outside its limit.

The Frequency, about once every shift, is based on operating experience that demonstrates the rarity of channel failure. Since the probability of two random failures in redundant channels in any 12 hour period is low, the CHANNEL CHECK minimizes the chance of loss of protective function due to failure of redundant channels. The CHANNEL CHECK supplements less formal, but more frequent, checks of channel OPERABILITY during normal operational use of the displays associated with the LCO required channels.

[For this plant, the CHANNEL CHECK verification of sample system alignment and operation for gaseous, particulate, iodine, and gamma monitors is as follows:]

SR 3.3.10.2

A CHANNEL FUNCTIONAL TEST is performed on the required fuel building radiation monitoring channel to ensure the entire channel will perform its intended function. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions. Any setpoint adjustment shall be consistent with the assumptions of the current plant specific setpoint analysis.

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the frequency extension analysis. The requirements for this review are outlined in Reference [4].

BASES

SURVEILLANCE REQUIREMENTS (continued)

The Frequency of 92 days is based on plant operating experience with regard to channel OPERABILITY and drift, which demonstrates that failure of more than one channel of a given Function in any 92 day Frequency is a rare event.

SR 3.3.10.3

Proper operation of the individual initiation relays is verified by actuating these relays during the CHANNEL FUNCTIONAL TEST of the Actuation Logic every [18] months. This will actuate the Function, operating all associated equipment. Proper operation of the equipment actuated by each train is thus verified. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions. The Frequency of [18] months is based on plant operating experience with regard to channel OPERABILITY and drift, which demonstrates that failure of more than one channel of a given Function during any [18] month Frequency is a rare event.

A Note to the SR indicates that this Surveillance includes verification of operation for each initiation relay.

[At this unit, the verification is conducted as follows:]

SR 3.3.10.4

Every 18 months, a CHANNEL FUNCTIONAL TEST is performed on the FHIS Manual Trip channel. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

BASES

SURVEILLANCE REQUIREMENTS (continued)

This Surveillance verifies that the trip push buttons are capable of opening contacts in the Actuation Logic as designed, de-energizing the initiation relays and providing Manual Trip of the Function. The [18] month Frequency is based on the need to perform this Surveillance under the conditions that apply during a plant outage and the potential for an unplanned transient if the Surveillance were performed with the reactor at power. Operating experience has shown these components usually pass the Surveillance when performed at a Frequency of once every [18] months.

SR 3.3.10.5

CHANNEL CALIBRATION is a complete check of the instrument channel including the sensor. The Surveillance verifies that the channel responds to a measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drift between successive calibrations to ensure that the channel remains operational between successive tests. CHANNEL CALIBRATIONS must be performed consistent with the plant specific setpoint analysis.

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the surveillance interval extension analysis. The requirements for this review are outlined in Reference [4].

The Frequency is based upon the assumption of an [18] month calibration interval for the determination of the magnitude of equipment drift in the setpoint analysis.

[SR 3.3.10.6

This Surveillance ensures that the train actuation response times are less than the maximum times assumed in the analyses. The [18] month Frequency is based upon plant operating experience, which shows that random failures of instrumentation components causing serious response time degradation, but not channel failure, are infrequent occurrences. Testing of the final actuating devices, which make up the bulk of the response time, is included in the Surveillance.]

BASES

REFERENCES

1. FSAR, Chapter [9].
2. FSAR, Chapter [15].
3. "Plant Protection System Selection of Trip Setpoint Values."
4. [ ].

B 3.3 INSTRUMENTATION

B 3.3.11 Post Accident Monitoring (PAM) Instrumentation (Digital)

BASES

BACKGROUND

The primary purpose of the PAM instrumentation is to display plant variables that provide information required by the control room operators during accident situations. This information provides the necessary support for the operator to take the manual actions, for which no automatic control is provided, that are required for safety systems to accomplish their safety functions for Design Basis Events.

The OPERABILITY of PAM instrumentation ensures that there is sufficient information available on selected plant parameters to monitor and assess plant status and behavior following an accident.

The availability of PAM instrumentation is important so that responses to corrective actions can be observed and the need for, and magnitude of, further actions can be determined. These essential instruments are identified by plant specific documents (Ref. 1) addressing the recommendations of Regulatory Guide 1.97 (Ref. 2), as required by Supplement 1 to NUREG-0737, "TMI Action Items" (Ref. 3).

Type A variables are included in this LCO because they provide the primary information required to permit the control room operator to take specific manually controlled actions, for which no automatic control is provided, that are required for safety systems to accomplish their safety functions for Design Basis Accidents (DBAs). Because the list of Type A variables differs widely between plants, Table 3.3.11-1 in the accompanying LCO contains no examples of Type A variables, except for those that may also be Category I.

Category I variables are the key variables deemed risk significant because they are needed to:

- Determine whether other systems important to safety are performing their intended functions,

- Provide information to the operators that will enable them to determine the potential for causing a gross breach of the barriers to radioactivity release, and

- Provide information regarding the release of radioactive materials to allow for early indication of the need to initiate action necessary to protect the public as well as to obtain an estimate of the magnitude of any impending threat.

BASES

BACKGROUND (continued)

These key variables are identified by plant specific Regulatory Guide 1.97 analyses (Ref. 1). These analyses identified the plant specific Type A variables and provided justification for deviating from the NRC proposed list of Category I variables.

----------------------------------REVIEWER'S NOTE----------------------------------
Table 3.3.11-1 provides a list of variables typical of those identified by plant specific Regulatory Guide 1.97 analyses. Table 3.3.11-1 in the plant specific Technical Specifications (TS) shall list all Type A and Category I variables identified by plant specific Regulatory Guide 1.97 analyses, as amended by the NRC's Safety Evaluation Report (SER) (Ref. 4). The specific instrument Functions listed in Table 3.3.11-1 are discussed in the LCO Bases.

APPLICABLE SAFETY ANALYSES

The PAM instrumentation ensures the OPERABILITY of Regulatory Guide 1.97 Type A variables, so that the control room operating staff can:

- Perform the diagnosis specified in the emergency operating procedures. These variables are restricted to preplanned actions for the primary success path of DBAs and
- Take the specified, preplanned, manually controlled actions, for which no automatic control is provided, that are required for safety systems to accomplish their safety functions.

The PAM instrumentation also ensures OPERABILITY of Category I, non-Type A variables. This ensures the control room operating staff can:

- Determine whether systems important to safety are performing their intended functions,
- Determine the potential for causing a gross breach of the barriers to radioactivity release,
- Determine if a gross breach of a barrier has occurred, and
- Initiate action necessary to protect the public as well as to obtain an estimate of the magnitude of any impending threat.

BASES

APPLICABLE SAFETY ANALYSES (continued)

PAM instrumentation that meets the definition of Type A in Regulatory Guide 1.97 satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

Category I, non-Type A PAM instruments are retained in the Specification because they are intended to assist operators in minimizing the consequences of accidents. Therefore, these Category I, non-Type A variables are important in reducing public risk.

LCO

LCO 3.3.11 requires two OPERABLE channels for all but one Function to ensure no single failure prevents the operators from being presented with the information necessary to determine the status of the plant and to bring the plant to, and maintain it in, a safe condition following that accident.

Furthermore, provision of two channels allows a CHANNEL CHECK during the post accident phase to confirm the validity of displayed information. [More than two channels may be required at some plants if the Regulatory Guide 1.97 analysis determined that failure of one accident monitoring channel results in information ambiguity (that is, the redundant displays disagree) that could lead operators to defeat or to fail to accomplish a required safety function.]

The exception to the two channel requirement is Penetration Flow Path Containment Isolation Valve Position. In this case, the important information is the status of the containment penetrations. The LCO requires one position indicator for each active containment isolation valve. This is sufficient to redundantly verify the isolation status of each isolable penetration either via indicated status of the active valve and prior knowledge of the passive valve or via system boundary status. If a normally active containment isolation valve is known to be closed and deactivated, position indication is not needed to determine status. Therefore, the position indication for valves in this state is not required to be OPERABLE.

Listed below are discussions of the specified instrument Functions listed in Table 3.3.11-1. These discussions are intended as examples of what should be provided for each Function when the plant specific list is prepared.

1. <u>[Wide Range] Neutron Flux</u>

   [Wide Range] Neutron Flux indication is provided to verify reactor shutdown.

   [At this unit, the [Wide Range] Neutron Flux PAM channels consist of the following:]

BASES

LCO (continued)

2, 3. Reactor Coolant System (RCS) Hot and Cold Leg Temperature

RCS Hot and Cold Leg Temperatures are Category I variables provided for verification of core cooling and long term surveillance.

Reactor outlet temperature inputs to the PAM are provided by two fast response resistance elements and associated transmitters in each loop. The channels provide indication over a range of 32°F to 700°F.

4. Reactor Coolant System Pressure (wide range)

RCS Pressure (wide range) is a Category I variable, provided for verification of core cooling and RCS integrity long term surveillance.

Wide range RCS loop pressure is measured by pressure transmitters with a span of 0 psig to 3000 psig. The pressure transmitters are located outside the containment. Redundant monitoring capability is provided by two trains of instrumentation. Control room indications are provided through the inadequate core cooling (ICC) plasma display. The ICC plasma display is the primary indication used by the operator during an accident. Therefore, the PAM instrumentation Specification deals specifically with this portion of the instrument channel.

In some plants, RCS pressure is a Type A variable because the operator uses this indication to monitor the cooldown of the RCS following a steam generator tube rupture or small break loss of coolant accident (LOCA). Operator actions to maintain a controlled cooldown, such as adjusting steam generator pressure or level, would use this indication. Furthermore, RCS pressure is one factor that may be used in decisions to terminate reactor coolant pump operation.

5. Reactor Vessel Water Level

Reactor Vessel Water Level is provided for verification and long term surveillance of core cooling.

BASES

LCO (continued)

The Reactor Vessel Water Level Monitoring System provides a direct measurement of the collapsed liquid level above the fuel alignment plate. The collapsed level represents the amount of liquid mass that is in the reactor vessel above the core. Measurement of the collapsed water level is selected because it is a direct indication of the water inventory. The collapsed level is obtained over the same temperature and pressure range as the saturation measurements, thereby encompassing all operating and accident conditions where it must function. Also, it functions during the recovery interval. Therefore, it is designed to survive the high steam temperature that may occur during the preceding core recovery interval.

The level range extends from the top of the vessel down to the top of the fuel alignment plate. The response time is short enough to track the level during small break LOCA events. The resolution is sufficient to show the initial level drop, the key locations near the hot leg elevation, and the lowest levels just above the alignment plate. This provides the operator with adequate indication to track the progression of the accident and to detect the consequences of its mitigating actions or the functionality of automatic equipment.

6. <u>Containment Sump Water Level (wide range)</u>

   Containment Sump Water Level is provided for verification and long term surveillance of RCS integrity.

   [For this unit, Containment Sump Water Level instrumentation consists of the following:]

7. <u>Containment Pressure (wide range)</u>

   Containment Pressure is provided for verification of RCS and containment OPERABILITY.

   [For this unit, Containment Pressure instrumentation consists of the following:]

8. <u>Penetration Flow Path Containment Isolation Valve Position</u>

   Penetration Flow Path Containment Isolation Valve (CIV) Position is provided for verification of containment OPERABILITY.

BASES

LCO (continued)

CIV position is provided for verification of containment integrity. In the case of CIV position, the important information is the isolation status of the containment penetration. The LCO requires one channel of valve position indication in the control room to be OPERABLE for each active CIV in a containment penetration flow path, i.e., two total channels of CIV position indication for a penetration flow path with two active valves. For containment penetrations with only one active CIV having control room indication, Note (b) requires a single channel of valve position indication to be OPERABLE. This is sufficient to redundantly verify the isolation status of each isolable penetration via indicated status of the active valve, as applicable, and prior knowledge of passive valve or system boundary status. If a penetration flow path is isolated, position indication for the CIV(s) in the associated penetration flow path is not needed to determine status. Therefore, the position indication for valves in an isolated penetration flow path is not required to be OPERABLE. Each penetration is treated separately and each penetration flow path is considered a separate function. Therefore, separate condition entry is allowed for each inoperable penetration flow path.

[For this unit, the CIV position PAM instrumentation consists of the following:]

9. <u>Containment Area Radiation (high range)</u>

Containment Area Radiation is provided to monitor for the potential of significant radiation releases and to provide release assessment for use by operators in determining the need to invoke site emergency plans.

[For this unit, Containment Area Radiation instrumentation consists of the following:]

10. <u>Pressurizer Level</u>

Pressurizer Level is used to determine whether to terminate safety injection (SI), if still in progress, or to reinitiate SI if it has been stopped. Knowledge of pressurizer water level is also used to verify the plant conditions necessary to establish natural circulation in the RCS and to verify that the plant is maintained in a safe shutdown condition.

[For this unit, Pressurizer Level instrumentation consists of the following:]

BASES

LCO (continued)

11. Steam Generator Water Level

Steam Generator Water Level is provided to monitor operation of decay heat removal via the steam generators. The Category I indication of steam generator level is the extended startup range level instrumentation. The extended startup range level covers a span of 6 inches to 394 inches above the lower tubesheet. The measured differential pressure is displayed in inches of water at 68°F. Temperature compensation of this indication is performed manually by the operator. Redundant monitoring capability is provided by two trains of instrumentation. The uncompensated level signal is input to the plant computer, a control room indicator, and the Emergency Feedwater (EFW) Control System.

At some plants, operator action is based on the control room indication of Steam Generator Water Level. The RCS response during a design basis small break LOCA is dependent on the break size. For a certain range of break sizes, the boiler condenser mode of heat transfer is necessary to remove decay heat. At these plants, extended startup range level is a Type A variable because the operator must manually raise and control the steam generator level to establish boiler condenser heat transfer. Operator action is initiated on a loss of subcooled margin. Feedwater flow is increased until the indicated extended startup range level reaches the boiler condenser setpoint.

12. Condensate Storage Tank (CST) Level

CST Level is provided to ensure water supply for EFW. The CST provides the ensured, safety grade water supply for the EFW System. The CST consists of two identical tanks connected by a common outlet header. Inventory is monitored by a 0 to 144 inch level indication for each tank. CST Level is displayed on a control room indicator, strip chart recorder, and plant computer. In addition, a control room annunciator alarms on low level.

At some plants, CST Level is considered a Type A variable because the control room meter and annunciator are considered the primary indication used by the operator. The DBAs that require EFW are the loss of electric power, steam line break (SLB), and small break LOCA. The CST is the initial source of water for the EFW System. However, as the CST is depleted, manual operator action is necessary to replenish the CST or align suction to the EFW pumps from the hotwell.

BASES

LCO (continued)

13, 14, 15, 16. Core Exit Temperature

Core Exit Temperature is provided for verification and long term surveillance of core cooling.

An evaluation was made of the minimum number of valid core exit thermocouples necessary for inadequate core cooling detection. The evaluation determined the reduced complement of core exit thermocouples necessary to detect initial core recovery and trend the ensuing core heatup. The evaluations account for core nonuniformities including incore effects of the radial decay power distribution and excore effects of condensate runback in the hot legs and nonuniform inlet temperatures. Based on these evaluations, adequate or inadequate core cooling detection is ensured with two valid core exit thermocouples per quadrant.

The design of the Incore Instrumentation System includes a Type K (chromel alumel) thermocouple within each of the 56 incore instrument detector assemblies. The junction of each thermocouple is located a few inches above the fuel assembly, inside a structure that supports and shields the incore instrument detector assembly string from flow forces in the outlet plenum region. These core exit thermocouples monitor the temperature of the reactor coolant as it exits the fuel assemblies.

The core exit thermocouples have a usable temperature range from 32°F to 2300°F, although accuracy is reduced at temperatures above 1800°F.

17. Emergency Feedwater (EFW) Flow

EFW Flow is provided to monitor operation of decay heat removal via the steam generators.

EFW Flow to each steam generator is determined from a differential pressure measurement calibrated to a span of 0 gpm to 1200 gpm. Redundant monitoring capability is provided by two independent trains of instrumentation for each steam generator. Each differential pressure transmitter provides an input to a control room indicator and the plant computer. Since the primary indication used by the operator during an accident is the control room indicator, the PAM instrumentation Specification deals specifically with this portion of the instrument channel.

BASES

LCO (continued)

> At some plants EFW Flow is a Type A variable because operator action is required to throttle flow during an SLB accident in order to prevent the EFW pumps from operating in runout conditions. EFW Flow is also used by the operator to verify that the EFW System is delivering the correct flow to each steam generator. However, the primary indication used by the operator to ensure an adequate inventory is steam generator level.

Two channels are required to be OPERABLE for all but one Function. Two OPERABLE channels ensure that no single failure within the PAM instrumentation or its auxiliary supporting features or power sources, concurrent with failures that are a condition of or result from a specific accident, prevents the operators from being presented the information necessary for them to determine the safety status of the plant and to bring the plant to and maintain it in a safe condition following that accident.

In Table 3.3.11-1 the exception to the two channel requirement is Containment Isolation Valve Position.

Two OPERABLE channels of core exit thermocouples are required for each channel in each quadrant to provide indication of radial distribution of the coolant temperature rise across representative regions of the core. Power distribution symmetry was considered in determining the specific number and locations provided for diagnosis of local core problems. Therefore, two randomly selected thermocouples may not be sufficient to meet the two thermocouples per channel requirement in any quadrant. The two thermocouples in each channel must meet the additional requirement that one be located near the center of the core and the other near the core perimeter, such that the pair of core exit thermocouples indicate the radial temperature gradient across their core quadrant. Plant specific evaluations in response to Item II.F.2 of NUREG-0737 (Ref. 3) should have identified the thermocouple pairings that satisfy these requirements. Two sets of two thermocouples in each quadrant ensure a single failure will not disable the ability to determine the radial temperature gradient.

For loop and steam generator related variables, the required information is individual loop temperature and individual steam generator level. In these cases two channels are required to be OPERABLE for each loop of steam generator to redundantly provide the necessary information.

BASES

LCO (continued)

In the case of Containment Isolation Valve Position, the important information is the status of the containment penetrations. The LCO requires one position indicator for each active containment isolation valve. This is sufficient to redundantly verify the isolation status of each isolable penetration either via indicated status of the active valve and prior knowledge of the passive valve or via system boundary status. If a normally active containment isolation valve is known to be closed and deactivated, position indication is not needed to determine status. Therefore, the position indication for valves in this state is not required to be OPERABLE.

APPLICABILITY

The PAM instrumentation LCO is applicable in MODES 1, 2, and 3. These variables are related to the diagnosis and preplanned actions required to mitigate DBAs. The applicable DBAs are assumed to occur in MODES 1, 2, and 3. In MODES 4, 5, and 6, plant conditions are such that the likelihood of an event occurring that would require PAM instrumentation is low; therefore, PAM instrumentation is not required to be OPERABLE in these MODES.

ACTIONS

A Note has been added in the ACTIONS to clarify the application of Completion Time rules. The Conditions of this Specification may be entered independently for each Function listed in Table 3.3.11-1. The Completion Time(s) of the inoperable channel(s) of a Function will be tracked separately for each Function starting from the time the Condition was entered for that Function.

A.1

When one or more Functions have one required channel that is inoperable, the required inoperable channel must be restored to OPERABLE status within 30 days. The 30 day Completion Time is based on operating experience and takes into account the remaining OPERABLE channel (or in the case of a Function that has only one required channel, other non-Regulatory Guide 1.97 instrument channels to monitor the Function), the passive nature of the instrument (no critical automatic action is assumed to occur from these instruments), and the low probability of an event requiring PAM instrumentation during this interval.

BASES

ACTIONS (continued)

B.1

This Required Action specifies initiation of actions in accordance with Specification 5.6.5, which requires a written report to be submitted to the Nuclear Regulatory Commission. This report discusses the results of the root cause evaluation of the inoperability and identifies proposed restorative Required Actions. This Required Action is appropriate in lieu of a shutdown requirement, given the likelihood of plant conditions that would require information provided by this instrumentation. Also, alternative Required Actions are identified before a loss of functional capability condition occurs.

C.1

When one or more Functions have two required channels inoperable (i.e., two channels inoperable in the same Function), one channel in the Function should be restored to OPERABLE status within 7 days. The Completion Time of 7 days is based on the relatively low probability of an event requiring PAM instrumentation operation and the availability of alternate means to obtain the required information. Continuous operation with two required channels inoperable in a Function is not acceptable because the alternate indications may not fully meet all performance qualification requirements applied to the PAM instrumentation. Therefore, requiring restoration of one inoperable channel of the Function limits the risk that the PAM Function will be in a degraded condition should an accident occur.

D.1

This Required Action directs entry into the appropriate Condition referenced in Table 3.3.11-1. The applicable Condition referenced in the Table is Function dependent. Each time Required Action C.1 is not met, and the associated Completion Time has expired, Condition D is entered for that channel and provides for transfer to the appropriate subsequent Condition.

BASES

ACTIONS (continued)

E.1 and E.2

If the Required Action and associated Completion Time of Condition C are not met and Table 3.3.11-1 directs entry into Condition E, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 4 within 12 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

[F.1

At this plant, alternate means of monitoring Reactor Vessel Water Level and Containment Area Radiation have been developed and tested. These alternate means may be temporarily installed if the normal PAM channel cannot be restored to OPERABLE status within the allotted time. If these alternate means are used, the Required Action is not to shut down the plant, but rather to follow the directions of Specification 5.6.5. The report provided to the NRC should discuss whether the alternate means are equivalent to the installed PAM channels, justify the areas in which they are not equivalent, and provide a schedule for restoring the normal PAM channels.]

SURVEILLANCE REQUIREMENTS

A Note at the beginning of the SR Table specifies thatthe following SRs apply to each PAM instrumentation Function found in Table 3.3.11-1.

SR 3.3.11.1

Performance of the CHANNEL CHECK once every 31 days ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the parameter indicated on one channel to a similar parameter on other channels. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value. Significant deviations between the two instrument channels could be an indication of excessive instrument drift in one of the channels or of something even more serious. A CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

BASES

SURVEILLANCE REQUIREMENTS (continued)

Agreement criteria are determined by the plant staff based on a combination of the channel instrument uncertainties, including indication and readability. If a channel is outside the criteria, it may be an indication that the sensor or the signal processing equipment has drifted outside its limit. If the channels are within the criteria, it is an indication that the channels are OPERABLE. If the channels are normally off scale during times when surveillance is required, the CHANNEL CHECK will only verify that they are off scale in the same direction. Off scale low current loop channels are verified to be reading at the bottom of the range and not failed downscale.

The Frequency of 31 days is based upon plant operating experience with regard to channel OPERABILITY and drift, which demonstrates that failure of more than one channel of a given Function in any 31 day interval is a rare event. The CHANNEL CHECK supplements less formal, but more frequent, checks of channel during normal operational use of the displays associated with this LCO's required channels.

SR 3.3.11.2

A CHANNEL CALIBRATION is performed every [18] months or approximately every refueling. CHANNEL CALIBRATION is a complete check of the instrument channel including the sensor. The Surveillance verifies the channel responds to the measured parameter within the necessary range and accuracy. A Note allows exclusion of the neutron detectors from the CHANNEL CALIBRATION.

[At this unit, CHANNEL CALIBRATION shall find measurement errors are within the following acceptance criteria:]

For the Containment Area Radiation instrumentation, a CHANNEL CALIBRATION may consist of an electronic calibration of the channel, not including the detector, for range decades above 10 R/hr, and a one point calibration check of the detector below 10 R/hr with a gamma source.

Whenever a sensing element is replaced, the next required CHANNEL CALIBRATION of the resistance temperature detectors (RTD) sensors is accomplished by an inplace cross calibration that compares the other sensing elements with the recently installed sensing element.

BASES

SURVEILLANCE REQUIREMENTS (continued)

Whenever a sensing element is replaced, the next required CHANNEL CALIBRATION of the Core Exit thermocouple sensors is accomplished by an inplace cross calibration that compares the other sensing elements with the recently installed sensing element.

The Frequency is based upon operating experience and consistency with the typical industry refueling cycle and is justified by the assumption of an [18] month calibration interval for the determination of the magnitude of equipment drift.

REFERENCES

[1. Plant specific document (e.g., FSAR, NRC Regulatory Guide 1.97, SER letter).]

2. Regulatory Guide 1.97.

3. NUREG-0737, Supplement 1.

4. NRC Safety Evaluation Report (SER).

B 3.3 INSTRUMENTATION

B 3.3.12 Remote Shutdown System (Digital)

BASES

BACKGROUND

The Remote Shutdown System provides the control room operator with sufficient instrumentation and controls to place and maintain the unit in a safe shutdown condition from a location other than the control room. This capability is necessary to protect against the possibility that the control room becomes inaccessible. A safe shutdown condition is defined as MODE 3. With the unit in MODE 3, the [Auxiliary Feedwater (AFW) System] and the steam generator safety valves or the steam generator atmospheric dump valves can be used to remove core decay heat and meet all safety requirements. The long term supply of water for the [AFW System] and the ability to borate the Reactor Coolant System (RCS) from outside the control room allow extended operation in MODE 3.

In the event that the control room becomes inaccessible, the operators can establish control at the remote shutdown panel and place and maintain the unit in MODE 3. Not all controls and necessary transfer switches are located at the remote shutdown panel. Some controls and transfer switches will be operated locally at the switchgear, motor control panels, or other local stations. The unit automatically reaches MODE 3 following a unit shutdown and can be maintained safely in MODE 3 for an extended period of time.

The OPERABILITY of the Remote Shutdown System control and instrumentation Functions ensures that there is sufficient information available on selected plant parameters to bring the plant to, and maintain it in, MODE 3 should the control room become inaccessible.

APPLICABLE SAFETY ANALYSES

The Remote Shutdown System is required to provide equipment at appropriate locations outside the control room with a capability to promptly shut down the plant and maintain it in a safe condition in MODE 3.

The criteria governing the design and the specific system requirements of the Remote Shutdown System are located in 10 CFR 50, Appendix A, GDC 19 (Ref. 1) and Appendix R (Ref. 2).

The Remote Shutdown System satisfies Criterion 4 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO	The Remote Shutdown System LCO provides the requirements for the OPERABILITY of the instrumentation and controls necessary to place and maintain the plant in MODE 3 from a location other than the control room. The instrumentation and controls required are listed in Table B 3.3.12-1.

The controls, instrumentation, and transfer switches are those required for:

- Reactivity Control (initial and long term),
- RCS Pressure Control,
- Decay Heat Removal,
- RCS Inventory Control, and
- Safety support systems for the above Functions, as well as service water, component cooling water, and onsite power including the diesel generators.

A Function of a Remote Shutdown System is OPERABLE if all instrument and control channels needed to support the remote shutdown Functions are OPERABLE. In some cases, Table B 3.3.12-1 may indicate that the required information or control capability is available from several alternate sources. In these cases, the Remote Shutdown System is OPERABLE as long as one channel of any of the alternate information or control sources for each Function is OPERABLE.

The Remote Shutdown System instrumentation and control circuits covered by this LCO do not need to be energized to be considered OPERABLE. This LCO is intended to ensure that the instrument and control circuits will be OPERABLE if plant conditions require that the Remote Shutdown System be placed in operation.

APPLICABILITY

The Remote Shutdown System LCO is applicable in MODES 1, 2, and 3. This is required so that the unit can be placed and maintained in MODE 3 for an extended period of time from a location other than the control room.

This LCO is not applicable in MODE 4, 5, or 6. In these MODES, the unit is already subcritical and in the condition of reduced RCS energy. Under these conditions, considerable time is available to restore necessary instrument control Functions if control room instruments or control become unavailable.

BASES

ACTIONS

A Remote Shutdown System division is inoperable when each Function is not accomplished by at least one designated Remote Shutdown System channel that satisfies the OPERABILITY criteria for the channel's Function. These criteria are outlined in the LCO section of the Bases.

A Note has been added in the ACTIONS to clarify the application of Completion Time rules. The Conditions of this Specification may be entered independently for each Function. The Completion Time(s) of the inoperable channel(s)/train(s) of a Function will be tracked separately for each Function starting from the time the Condition was entered for that Function.

A.1

Condition A addresses the situation where one or more channels of the Remote Shutdown System are inoperable. This includes the control and transfer switches for any required Function.

The Required Action is to restore the divisions to OPERABLE status within 30 days. The Completion Time is based on operating experience and the low probability of an event that would require evacuation of the control room.

B.1 and B.2

If the Required Action and associated Completion Time of Condition A are not met, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 4 within [12] hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required MODE from full power conditions in an orderly manner and without challenging plant systems.

BASES

SURVEILLANCE REQUIREMENTS

[SR 3.3.12.1

Performance of the CHANNEL CHECK once every 31 days ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the parameter indicated on one channel to a similar parameter on other channels. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value. Significant deviations between the instrument channels could be an indication of excessive instrument drift in one of the channels or of something even more serious. A CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying that the instrumentation continues to operate properly between each CHANNEL CALIBRATION. Agreement criteria are determined by the plant staff, based on a combination of the channel instrument uncertainties, including indication and readability. If a channel is outside the criteria, it may be an indication that the sensor or the signal processing equipment has drifted outside its limit. As specified in the Surveillance, a CHANNEL CHECK is only required for those channels that are normally energized.

The Frequency is based on plant operating experience that demonstrates channel failure is rare.]

SR 3.3.12.2

SR 3.3.12.2 verifies that each required Remote Shutdown System transfer switch and control circuit performs its intended function. This verification is performed from the reactor shutdown panel and locally, as appropriate. Operation of the equipment from the remote shutdown panel is not necessary. The Surveillance can be satisfied by performance of a continuity check. This will ensure that if the control room becomes inaccessible, the plant can be brought to and maintained in MODE 3 from the reactor shutdown panel and the local control stations. The [18] month Frequency is based on the need to perform this Surveillance under the conditions that apply during a plant outage and the potential for an unplanned transient if the Surveillance were performed with the reactor at power. Operating experience demonstrates that Remote Shutdown System control channels seldom fail to pass the Surveillance when performed at a Frequency of once every [18] months.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.12.3

CHANNEL CALIBRATION is a complete check of the instrument channel including the sensor. The Surveillance verifies that the channel responds to the measured parameter within the necessary range and accuracy. Whenever a sensing element is replaced, the next required CHANNEL CALIBRATION of the resistance temperature detectors (RTD) sensors is accomplished by an inplace cross calibration that compares the other sensing elements with the recently installed sensing element.

The [18] month Frequency is based on the need to perform this Surveillance under the conditions that apply during a plant outage and the potential for an unplanned transient if the Surveillance were performed with the reactor at power.

[SR 3.3.12.4

SR 3.3.12.4 is the performance of a CHANNEL FUNCTIONAL TEST every 18 months. This Surveillance should verify the OPERABILITY of the reactor trip circuit breaker (RTCB) open/closed indication on the remote shutdown panels by actuating the RTCBs. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions. The Frequency of 18 months was chosen because the RTCBs cannot be exercised while the unit is at power. Operating experience has shown that these components usually pass the Surveillance when performed at a Frequency of once every 18 months. Therefore, the Frequency was concluded to be acceptable from a reliability standpoint.]

REFERENCES

1. 10 CFR 50, Appendix A, GDC 19.

2. 10 CFR 50, Appendix R.

3. NRC Safety Evaluation Report (SER).

Table B 3.3.12-1 (page 1 of 1)
Remote Shutdown System Instrumentation and Controls

--NOTE--
This Table is for illustration purposes only. It does not attempt to encompass every Function used at every unit, but does contain the types of Functions commonly found.

FUNCTION/INSTRUMENT OR CONTROL PARAMETER	REQUIRED NUMBER OF DIVISIONS
1. Reactivity Control	
a. Log Power Neutron Flux	[1]
b. Source Range Neutron Flux	[1]
c. Reactor Trip Circuit Breaker Position	[1 per trip breaker]
d. Manual Reactor Trip	[4]
2. Reactor Coolant System Pressure Control	
a. Pressurizer Pressure or RCS Wide Range Pressure	[1]
b. Pressurizer Power Operated Relief Valve Control and Block Valve Control	[1, controls must be for power operated relief valve and block valves on same line]
3. Decay Heat Removal via Steam Generators	
a. Reactor Coolant\ Hot Leg Temperature	[1 per loop]
b. Reactor Coolant Cold Leg Temperature	[1 per loop]
c. Auxiliary Feedwater Controls	[1]
d. Steam Generator Pressure	[1 per steam generator]
e. Steam Generator Level or Auxiliary Feedwater Flow	[1 per steam generator]
f. Condensate Storage Tank Level	[1]
4. Reactor Coolant System Inventory Control	
a. Pressurizer Level	[1]
b. Reactor Coolant Charging Pump Controls	[1]

---REVIEWER'S NOTE---
The number of channels that fulfill GDC 19 requirements for the number of OPERABLE channels required depends upon the plant's licensing basis as described in the NRC plant specific Safety Evaluation Report (SER) (Ref. 3). Generally, two divisions are required to be OPERABLE. However, only one channel is required if the plant has justified such a design and the NRC's SER accepted the justification.

B 3.3 INSTRUMENTATION

B 3.3.13 [Logarithmic] Power Monitoring Channels (Digital)

BASES

BACKGROUND

The [logarithmic] power monitoring channels provide neutron flux power indication from < 1E-7% RTP to > 100% RTP. They also provide reactor protection when the reactor trip circuit breakers (RTCBs) are shut, in the form of a Power Rate of Change - High trip (analog plants) or a [Logarithmic] Power Level - High trip (digital plants).

This LCO addresses MODES 3, 4, and 5 with the RTCBs open. When the RTCBs are shut, the [logarithmic] power monitoring channels are addressed by LCO 3.3.2, "Reactor Protective System (RPS) Instrumentation - Shutdown."

When the RTCBs are open, two of the four wide range power channels must be available to monitor neutron flux power. In this application, the RPS channels need not be OPERABLE since the reactor trip Function is not required. By monitoring neutron flux (wide range) power when the RTCBs are open, loss of SDM caused by boron dilution can be detected as an increase in flux. Alarms are also provided when power increases above the fixed bistable setpoints. For plants employing separate post accident, wide range nuclear instrumentation channels with adequate range, these can be substituted for the [logarithmic] power range channels. Two channels must be OPERABLE to provide single failure protection and to facilitate detection of channel failure by providing CHANNEL CHECK capability.

APPLICABLE SAFETY ANALYSES

The [logarithmic] power monitoring channels are necessary to monitor core reactivity changes. They are the primary means for detecting and triggering operator actions to respond to reactivity transients initiated from conditions in which the RPS is not required to be OPERABLE. They also trigger operator actions to anticipate RPS actuation in the event of reactivity transients starting from shutdown or low power conditions. The [logarithmic] power monitoring channel's LCO requirements support compliance with 10 CFR 50, Appendix A, GDC 13 (Ref. 1). Reference 2 describes the specific [logarithmic] power monitoring channel features that are critical to comply with the GDC.

The OPERABILITY of [logarithmic] power monitoring channels is necessary to meet the assumptions of the safety analyses and provide for the mitigation of accident and transient conditions.

The [logarithmic] power monitoring channels satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO

The LCO on the [logarithmic] power monitoring channels ensures that adequate information is available to verify core reactivity conditions while shut down.

A minimum of two [logarithmic] power monitoring channels are required to be OPERABLE. Some plants may have four or six channels capable of performing this function. In these cases, multiple failures may be tolerated while the plants are still complying with LCO requirements.

APPLICABILITY

In MODES 3, 4, and 5, with RTCBs open or the Control Element Assembly (CEA) Drive System not capable of CEA withdrawal, [logarithmic] power monitoring channels must be OPERABLE to monitor core power for reactivity changes. In MODES 1 and 2, and in MODES 3, 4, and 5, with the RTCBs shut and the CEAs capable of withdrawal, the [logarithmic] power monitoring channels are addressed as part of the RPS in LCO 3.3.1, "Reactor Protective System (RPS) Instrumentation - Operating."

The requirements for source range neutron flux monitoring in MODE 6 are addressed in LCO 3.9.2, "Nuclear Instrumentation." The source range nuclear instrumentation channels provide neutron flux coverage extending an additional one to two decades below the [logarithmic] channels for use during refueling, when neutron flux may be extremely low. They are built into the [wide range] neutron flux channels in the analog plants and in many of the post accident channels used in both the digital and analog plants.

ACTIONS

A channel is inoperable when it does not satisfy the OPERABILITY criteria for the channel's function. These criteria are outlined in the LCO section of the Bases.

<u>A.1 and A.2</u>

With one required channel inoperable, it may not be possible to perform a CHANNEL CHECK to verify that the other required channel is OPERABLE. Therefore, with one or more required channels inoperable, the [logarithmic] power monitoring Function cannot be reliably performed. Consequently, the Required Actions are the same for one required channel inoperable or more than one required channel inoperable. The absence of reliable neutron flux indication makes it difficult to ensure SDM is maintained. Required Action [A.1] is modified by a Note to indicate that normal plant control operations that individually add limited positive reactivity (e.g., temperature or boron fluctuations associated with RCS inventory management or temperature control) are not precluded by this Action, provided they are accounted for in the calculated SDM.

BASES

ACTIONS (continued)

SDM must be verified periodically to ensure that it is being maintained. Both required channels must be restored as soon as possible. The initial Completion Time of 4 hours and once every 12 hours thereafter to perform SDM verification takes into consideration that Required Action A.1 eliminates many of the means by which SDM can be reduced. These Completion Times are also based on operating experience in performing the Required Actions and the fact that plant conditions will change slowly.

SURVEILLANCE REQUIREMENTS

SR 3.3.13.1

SR 3.3.13.1 is the performance of a CHANNEL CHECK on each required channel every 12 hours. A CHANNEL CHECK is normally a comparison of the parameter indicated on one channel to a similar parameter on other channels. It is based upon the assumption that instrument channels monitoring the same parameter should read approximately the same value. Significant deviations between instrument channels could be an indication of excessive instrument drift in one of the channels or of something even more serious. CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying that the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

Agreement criteria are determined by the plant staff and should be based on a combination of the channel instrument uncertainties including control isolation, indication, and readability. If a channel is outside of the criteria, it may be an indication that the transmitter or the signal processing equipment has drifted outside of its limits. If the channels are within the criteria, it is an indication that the channels are OPERABLE.

The Frequency, about once every shift, is based on operating experience that demonstrates the rarity of channel failure. Since the probability of two random failures in redundant channels in any 12 hour period is extremely low, CHANNEL CHECK minimizes the chance of loss of protective function due to failure of redundant channels. CHANNEL CHECK supplements less formal, but more frequent, checks of channel OPERABILITY during normal operational use of displays associated with the LCO required channels.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.13.2

A CHANNEL FUNCTIONAL TEST is performed every [92] days to ensure that the entire channel is capable of properly indicating neutron flux. Internal test circuitry is used to feed preadjusted test signals into the preamplifier to verify channel alignment. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions. It is not necessary to test the detector, because generating a meaningful test signal is difficult; the detectors are of simple construction, and any failures in the detectors will be apparent as change in channel output. This Frequency is the same as that employed for the same channels in the other applicable MODES.

[At this unit, the channel trip Functions tested by the CHANNEL FUNCTIONAL TEST are as follows:]

SR 3.3.13.3

SR 3.3.13.3 is the performance of a CHANNEL CALIBRATION. A CHANNEL CALIBRATION is performed every [18] months. The Surveillance is a complete check and readjustment of the [logarithmic] power channel from the preamplifier input through to the remote indicators. The Surveillance verifies that the channel responds to a measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drift between successive calibrations to ensure that the channel remains operational. CHANNEL CALIBRATIONS must be performed consistent with the plant specific setpoint analysis.

This SR is modified by a Note to indicate that it is not necessary to test the detector, because generating a meaningful test signal is difficult; the detectors are of simple construction, and any failures in the detectors will be apparent as change in channel output. This test interval is the same as that employed for the same channels in the other applicable MODES.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 13.

2. FSAR, Chapter [7] and Chapter [15].

B 3.4 REACTOR COOLANT SYSTEM (RCS)

B 3.4.1 RCS Pressure, Temperature, and Flow [Departure from Nucleate Boiling (DNB)] Limits

BASES

BACKGROUND

These Bases address requirements for maintaining RCS pressure, temperature, and flow rate within limits assumed in the safety analyses. The safety analyses (Ref. 1) of normal operating conditions and anticipated operational occurrences assume initial conditions within the normal steady state envelope. The limits placed on departure from nucleate boiling (DNB) related parameters ensure that these parameters will not be less conservative than were assumed in the analyses and thereby provide assurance that the minimum departure from nucleate boiling ratio (DNBR) will meet the required criteria for each of the transients analyzed.

The LCO limits for minimum and maximum RCS pressures as measured at the pressurizer are consistent with operation within the nominal operating envelope and are bounded by those used as the initial pressures in the analyses.

The LCO limits for minimum and maximum RCS cold leg temperatures are consistent with operation at the indicated power level and are bounded by those used as the initial temperatures in the analyses.

The LCO limits for minimum RCS flow rate is bounded by the initial flow rate in the analyses. The RCS flow rate is not expected to vary during plant operation with all pumps running.

APPLICABLE SAFETY ANALYSES

The requirements of LCO 3.4.1 represent the initial conditions for DNB limited transients analyzed in the safety analyses (Ref. 1). The safety analyses have shown that transients initiated from the limits of this LCO will meet the DNBR criterion of ≥ [1.3]. This is the acceptance limit for the RCS DNB parameters. Changes to the facility that could impact these parameters must be assessed for their impact on the DNBR criterion. The transients analyzed for include loss of coolant flow events and dropped or struck control element assembly (CEA) events. A key assumption for the analysis of these events is that the core power distribution is within the limits of [LCO 3.1.6, "Regulating CEA Insertion Limits," LCO 3.1.7, "Part Length CEA Insertion Limits," LCO 3.2.3, "AZIMUTHAL POWER TILT (Tq)," and LCO 3.2.5, "AXIAL SHAPE INDEX (ASI)"]. The safety analyses are performed over the following range of initial values: RCS pressure [1785-2400] psig, core inlet temperature [500-580]°F, and reactor vessel inlet coolant flow rate > [95]%.

The RCS DNB limits satisfy Criterion 2 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO	This LCO specifies limits on the monitored process variables - RCS pressurizer pressure, RCS cold leg temperature, and RCS total flow rate - to ensure that the core operates within the limits assumed for the plant safety analyses. Operating within these limits will result in meeting the DNBR criterion in the event of a DNB limited transient. The LCO numerical values for pressure, temperature, and flow rate are given for the measurement location but have not been adjusted for instrument error. Plant specific limits of instrument error are established by the plant staff to meet the operational requirements of this LCO.
APPLICABILITY	In MODE 1, the limits on RCS pressurizer pressure, RCS cold leg temperature, and RCS flow rate must be maintained during steady state operation in order to ensure that DNBR criteria will be met in the event of an unplanned loss of forced coolant flow or other DNB limited transient. In all other MODES, the power level is low enough so that DNBR is not a concern. A Note has been added to indicate the limit on pressurizer pressure may be exceeded during short term operational transients such as a THERMAL POWER ramp increase of > 5% RTP per minute or a THERMAL POWER step increase of > 10% RTP. These conditions represent short term perturbations where actions to control pressure variations might be counterproductive. Also, since they represent transients initiated from power levels < 100% RTP, an increased DNBR margin exists to offset the temporary pressure variations. Another set of limits on DNB related parameters is provided in Safety Limit (SL) 2.1.1, "Reactor Core Safety Limits." Those limits are less restrictive than the limits of this LCO, but violation of SLs merits a stricter, more severe Required Action. Should a violation of this LCO occur, the operator should check whether or not an SL may have been exceeded.
ACTIONS	<u>A.1</u> Pressurizer pressure is a controllable and measurable parameter. RCS flow rate is not a controllable parameter and is not expected to vary during steady state operation. With either parameter not within the LCO limits, action must be taken to restore the out of limit parameter. The 2 hour Completion Time for restoration of the parameters provides sufficient time to adjust plant parameters, to determine the cause of the off normal condition, and to restore the readings within limits. The Completion Time is based on plant operating experience that shows the parameter can be restored in this time period.

BASES

ACTIONS (continued)

B.1

If Required Action A.1 is not met within the associated Completion Time, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 2 within 6 hours. In MODE 2, the reduced power condition eliminates the potential for violation of the accident analysis bounds.

Six hours is a reasonable time that permits the plant power to be reduced at an orderly rate in conjunction with even control of steam generator (SG) heat removal.

C.1

Cold leg temperature is a controllable and measurable parameter. If this parameter is not within the LCO limits, action must be taken to restore the parameter.

The 2 hour Completion Time is based on plant operating experience that shows that the parameter can be restored in this time period.

D.1

If Required Action C.1 is not met within the associated Completion Time, THERMAL POWER must be reduced to ≤ [30%] RTP. Plant operation may continue for an indefinite period of time in this condition. At the reduced power level, the potential for violation of the DNB limits is greatly reduced.

The 6 hour Completion Time is a reasonable time that permits power reduction at an orderly rate in conjunction with even control of SG heat removal.

SURVEILLANCE REQUIREMENTS

SR 3.4.1.1

Since Required Action A.1 allows a Completion Time of 2 hours to restore parameters that are not within limits, the 12 hour Surveillance Frequency for pressurizer pressure is sufficient to ensure that the pressure can be restored to a normal operation, steady state condition following load changes and other expected transient operations. The 12 hour interval has been shown by operating practice to be sufficient to regularly assess for potential degradation and verify operation is within safety analysis assumptions.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.4.1.2

Since Required Action A.1 allows a Completion Time of 2 hours to restore parameters that are not within limits, the 12 hour Surveillance Frequency for cold leg temperature is sufficient to ensure that the RCS coolant temperature can be restored to a normal operation, steady state condition following load changes and other expected transient operations. The 12 hour interval has been shown by operating practice to be sufficient to regularly assess for potential degradation and to verify operation is within safety analysis assumptions.

SR 3.4.1.3

The 12 hour Surveillance Frequency for RCS total flow rate is performed using the installed flow instrumentation. The 12 hour Frequency has been shown by operating experience to be sufficient to assess for potential degradation and to verify operation is within safety analysis assumptions.

This SR is modified by a Note that only requires performance of this SR in MODE 1. The Note is necessary to allow measurement of RCS flow rate at normal operating conditions at power with all RCPs running.

SR 3.4.1.4

Measurement of RCS total flow rate by performance of a precision calorimetric heat balance once every [18] months. This allows the installed RCS flow instrumentation to be calibrated and verifies that the actual RCS flow rate is within the bounds of the analyses.

The Frequency of [18] months reflects the importance of verifying flow after a refueling outage where the core has been altered, which may have caused an alteration of flow resistance.

The SR is modified by a Note that states the SR is only required to be performed [24] hours after ≥ [90]% RTP. The Note is necessary to allow measurement of the flow rate at normal operating conditions at power in MODE 1. The Surveillance cannot be performed in MODE 2 or below, and will not yield accurate results if performed below 90% RTP.

REFERENCES

1. FSAR, Section [15].

B 3.4 REACTOR COOLANT SYSTEM (RCS)

B 3.4.2 RCS Minimum Temperature for Criticality

BASES

BACKGROUND

Establishing the value for the minimum temperature for reactor criticality is based upon considerations for:

a. Operation within the existing instrumentation ranges and accuracies,

b. Operation within the bounds of the existing accident analyses, and

c. Operation with the reactor vessel above its minimum nil ductility reference temperature when the reactor is critical.

The reactor coolant moderator temperature coefficient used in core operating and accident analysis is typically defined for the normal operating temperature range (532°F to 573°F). The Reactor Protection System receives inputs from the narrow range hot leg temperature detectors, which have a range of 520°F to 620°F. The RCS loop average temperature (T_{avg}) is controlled using inputs of the same range. Nominal T_{avg} for making the reactor critical is 532°F. Safety and operating analyses for lower temperature have not been made.

APPLICABLE SAFETY ANALYSES

There are no accident analyses that dictate the minimum temperature for criticality, but all low power safety analyses assume initial temperatures near the [520]°F limit (Ref. 1).

The RCS minimum temperature for criticality satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

The purpose of the LCO is to prevent criticality outside the normal operating regime (532°F to 573°F) and to prevent operation in an unanalyzed condition.

The LCO is only applicable below [535]°F and provides a reasonable distance to the limit of [520]°F. This allows adequate time to trend its approach and take corrective actions prior to exceeding the limit.

APPLICABILITY

The reactor has been designed and analyzed to be critical in MODES 1 and 2 only and in accordance with this specification. Criticality is not permitted in any other MODE. Therefore, this LCO is applicable in MODE 1, and MODE 2 when $K_{eff} \geq 1.0$. Coupled with the applicability definition for criticality is a temperature limit. Monitoring is required at or below a T_{avg} of [535]°F. The no load temperature of 544°F is maintained by the Steam Dump Control System.

BASES

ACTIONS	<u>A.1</u> If T_{avg} is below [520]°F, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to MODE 2 with K_{eff} < 1.0 within 30 minutes. Rapid reactor shutdown can be readily and practically achieved within a 30 minute period. The allowed time reflects the ability to perform this action and to maintain the plant within the analyzed range.
SURVEILLANCE REQUIREMENTS	<u>SR 3.4.2.1</u> RCS loop average temperature is required to be verified at or above [520]°F every 12 hours. The SR to verify RCS loop average temperatures every 12 hours takes into account indications and alarms that are continuously available to the operator in the control room and is consistent with other routine Surveillances which are typically performed once per shift. In addition, operators are trained to be sensitive to RCS temperature during approach to criticality and will ensure that the minimum temperature for criticality is met as criticality is approached.
REFERENCES	1. FSAR, Section [15].

B 3.4 REACTOR COOLANT SYSTEM (RCS)

B 3.4.3 RCS Pressure and Temperature (P/T) Limits

BASES

BACKGROUND

All components of the RCS are designed to withstand effects of cyclic loads due to system pressure and temperature changes. These loads are introduced by startup (heatup) and shutdown (cooldown) operations, power transients, and reactor trips. This LCO limits the pressure and temperature changes during RCS heatup and cooldown, within the design assumptions and the stress limits for cyclic operation.

The PTLR contains P/T limit curves for heatup, cooldown, and inservice leak and hydrostatic (ISLH) testing, and data for the maximum rate of change of reactor coolant temperature (Ref. 1).

Each P/T limit curve defines an acceptable region for normal operation. The usual use of the curves is operational guidance during heatup or cooldown maneuvering, when pressure and temperature indications are monitored and compared to the applicable curve to determine that operation is within the allowable region.

The LCO establishes operating limits that provide a margin to brittle failure of the reactor vessel and piping of the reactor coolant pressure boundary (RCPB). The vessel is the component most subject to brittle failure, and the LCO limits apply mainly to the vessel. The limits do not apply to the pressurizer, which has different design characteristics and operating functions.

10 CFR 50, Appendix G (Ref. 2), requires the establishment of P/T limits for material fracture toughness requirements of the RCPB materials. Reference 2 requires an adequate margin to brittle failure during normal operation, anticipated operational occurrences, and system hydrostatic tests. It mandates the use of the ASME Code, Section III, Appendix G (Ref. 3).

The actual shift in the RT_{NDT} of the vessel material will be established periodically by removing and evaluating the irradiated reactor vessel material specimens, in accordance with ASTM E 185 (Ref. 4) and Appendix H of 10 CFR 50 (Ref. 5). The operating P/T limit curves will be adjusted, as necessary, based on the evaluation findings and the recommendations of Reference 3.

BASES

BACKGROUND (continued)

The P/T limit curves are composite curves established by superimposing limits derived from stress analyses of those portions of the reactor vessel and head that are the most restrictive. At any specific pressure, temperature, and temperature rate of change, one location within the reactor vessel will dictate the most restrictive limit. Across the span of the P/T limit curves, different locations are more restrictive, and, thus, the curves are composites of the most restrictive regions.

The heatup curve represents a different set of restrictions than the cooldown curve because the directions of the thermal gradients through the vessel wall are reversed. The thermal gradient reversal alters the location of the tensile stress between the outer and inner walls.

The criticality limit includes the Reference 2 requirement that the limit be no less than 40°F above the heatup curve or the cooldown curve and not less than the minimum permissible temperature for the ISLH testing. However, the criticality limit is not operationally limiting; a more restrictive limit exists in LCO 3.4.2, "RCS Minimum Temperature for Criticality."

The consequence of violating the LCO limits is that the RCS has been operated under conditions that can result in brittle failure of the RCPB, possibly leading to a nonisolable leak or loss of coolant accident. In the event these limits are exceeded, an evaluation must be performed to determine the effect on the structural integrity of the RCPB components. The ASME Code, Section XI, Appendix E (Ref. 6), provides a recommended methodology for evaluating an operating event that causes an excursion outside the limits.

APPLICABLE SAFETY ANALYSES

The P/T limits are not derived from Design Basis Accident (DBA) Analyses. They are prescribed during normal operation to avoid encountering pressure, temperature, and temperature rate of change conditions that might cause undetected flaws to propagate and cause nonductile failure of the RCPB, an unanalyzed condition. Reference 1 establishes the methodology for determining the P/T limits. Since the P/T limits are not derived from any DBA, there are no acceptance limits related to the P/T limits. Rather, the P/T limits are acceptance limits themselves since they preclude operation in an unanalyzed condition.

The RCS P/T limits satisfy Criterion 2 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO

The two elements of this LCO are:

a. The limit curves for heatup, cooldown, and ISLH testing and

b. Limits on the rate of change of temperature.

The LCO limits apply to all components of the RCS, except the pressurizer.

These limits define allowable operating regions and permit a large number of operating cycles while providing a wide margin to nonductile failure.

The limits for the rate of change of temperature control the thermal gradient through the vessel wall and are used as inputs for calculating the heatup, cooldown, and ISLH testing P/T limit curves. Thus, the LCO for the rate of change of temperature restricts stresses caused by thermal gradients and also ensures the validity of the P/T limit curves.

Violating the LCO limits places the reactor vessel outside of the bounds of the stress analyses and can increase stresses in other RCPB components. The consequences depend on several factors, as follows:

a. The severity of the departure from the allowable operating P/T regime or the severity of the rate of change of temperature,

b. The length of time the limits were violated (longer violations allow the temperature gradient in the thick vessel walls to become more pronounced), and

c. The existences, sizes, and orientations of flaws in the vessel material.

APPLICABILITY

The RCS P/T limits Specification provides a definition of acceptable operation for prevention of nonductile failure in accordance with 10 CFR 50, Appendix G (Ref. 2). Although the P/T limits were developed to provide guidance for operation during heatup or cooldown (MODES 3, 4, and 5) or ISLH testing, their Applicability is at all times in keeping with the concern for nonductile failure. The limits do not apply to the pressurizer.

During MODES 1 and 2, other Technical Specifications provide limits for operation that can be more restrictive than or can supplement these P/T limits. LCO 3.4.1, "RCS Pressure, Temperature, and Flow Departure from Nucleate Boiling (DNB) Limits," LCO 3.4.2, "RCS Minimum

BASES

APPLICABILITY (continued)

Temperature for Criticality," and Safety Limit 2.1, "Safety Limits," also provide operational restrictions for pressure and temperature and maximum pressure. Furthermore, MODES 1 and 2 are above the temperature range of concern for nonductile failure, and stress analyses have been performed for normal maneuvering profiles, such as power ascension or descent.

The actions of this LCO consider the premise that a violation of the limits occurred during normal plant maneuvering. Severe violations caused by abnormal transients, at times accompanied by equipment failures, may also require additional actions from emergency operating procedures.

ACTIONS

A.1 and A.2

Operation outside the P/T limits must be corrected so that the RCPB is returned to a condition that has been verified by stress analyses.

The 30 minute Completion Time reflects the urgency of restoring the parameters to within the analyzed range. Most violations will not be severe, and the activity can be accomplished in this time in a controlled manner.

Besides restoring operation to within limits, an evaluation is required to determine if RCS operation can continue. The evaluation must verify the RCPB integrity remains acceptable and must be completed before continuing operation. Several methods may be used, including comparison with pre-analyzed transients in the stress analyses, new analyses, or inspection of the components.

ASME Code, Section XI, Appendix E (Ref. 6), may be used to support the evaluation. However, its use is restricted to evaluation of the vessel beltline.

The 72 hour Completion Time is reasonable to accomplish the evaluation. The evaluation for a mild violation is possible within this time, but more severe violations may require special, event specific stress analyses or inspections. A favorable evaluation must be completed before continuing to operate.

Condition A is modified by a Note requiring Required Action A.2 to be completed whenever the Condition is entered. The Note emphasizes the need to perform the evaluation of the effects of the excursion outside the allowable limits. Restoration alone per Required Action A.1 is insufficient because higher than analyzed stresses may have occurred and may have affected the RCPB integrity.

BASES

ACTIONS (continued)

B.1 and B.2

If a Required Action and associated Completion Time of Condition A are not met, the plant must be placed in a lower MODE because:

a. The RCS remained in an unacceptable P/T region for an extended period of increased stress or

b. A sufficiently severe event caused entry into an unacceptable region.

Either possibility indicates a need for more careful examination of the event, best accomplished with the RCS at reduced pressure and temperature. With reduced pressure and temperature conditions, the possibility of propagation of undetected flaws is decreased.

Pressure and temperature are reduced by placing the plant in MODE 3 within 6 hours and in MODE 5 with RCS pressure < [500] psig within 36 hours.

The Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

C.1 and C.2

The actions of this LCO, anytime other than in MODE 1, 2, 3, or 4, consider the premise that a violation of the limits occurred during normal plant maneuvering. Severe violations caused by abnormal transients, at times accompanied by equipment failures, may also require additional actions from emergency operating procedures. Operation outside the P/T limits must be corrected so that the RCPB is returned to a condition that has been verified by stress analyses.

The Completion Time of "immediately" reflects the urgency of restoring the parameters to within the analyzed range. Most violations will not be severe, and the activity can be accomplished in a short period of time in a controlled manner.

Besides restoring operation to within limits, an evaluation is required to determine if RCS operation can continue. The evaluation must verify that the RCPB integrity remains acceptable and must be completed before continuing operation. Several methods may be used, including comparison with pre-analyzed transients in the stress analyses, new analyses, or inspection of the components.

BASES

ACTIONS (continued)

ASME Code, Section XI, Appendix E (Ref. 6), may be used to support the evaluation. However, its use is restricted to evaluation of the vessel beltline.

The Completion Time of prior to entering MODE 4 forces the evaluation prior to entering a MODE where temperature and pressure can be significantly increased. The evaluation for a mild violation is possible within several days, but more severe violations may require special, event specific stress analyses or inspections.

Condition C is modified by a Note requiring Required Action C.2 to be completed whenever the Condition is entered. The Note emphasizes the need to perform the evaluation of the effects of the excursion outside the allowable limits. Restoration alone per Required Action C.1 is insufficient because higher than analyzed stresses may have occurred and may have affected the RCPB integrity.

SURVEILLANCE REQUIREMENTS

SR 3.4.3.1

Verification that operation is within the PTLR limits is required every 30 minutes when RCS pressure and temperature conditions are undergoing planned changes. This Frequency is considered reasonable in view of the control room indication available to monitor RCS status. Also, since temperature rate of change limits are specified in hourly increments, 30 minutes permits assessment and correction for minor deviations within a reasonable time.

Surveillance for heatup, cooldown, or ISLH testing may be discontinued when the definition given in the relevant plant procedure for ending the activity is satisfied.

This SR is modified by a Note that requires this SR be performed only during RCS system heatup, cooldown, and ISLH testing. No SR is given for criticality operations because LCO 3.4.2 contains a more restrictive requirement.

BASES

REFERENCES

1. [NRC approved topical report that defines the methodology for determining the P/T limits].
2. 10 CFR 50, Appendix G.
3. ASME, Boiler and Pressure Vessel Code, Section III, Appendix G.
4. ASTM E 185-82, July 1982.
5. 10 CFR 50, Appendix H.
6. ASME, Boiler and Pressure Vessel Code, Section XI, Appendix E.

B 3.4 REACTOR COOLANT SYSTEM (RCS)

B 3.4.4 RCS Loops - MODES 1 and 2

BASES

BACKGROUND

The primary function of the RCS is removal of the heat generated in the fuel due to the fission process and transfer of this heat, via the steam generators (SGs), to the secondary plant.

The secondary functions of the RCS include:

a. Moderating the neutron energy level to the thermal state, to increase the probability of fission,

b. Improving the neutron economy by acting as a reflector,

c. Carrying the soluble neutron poison, boric acid,

d. Providing a second barrier against fission product release to the environment, and

e. Removing the heat generated in the fuel due to fission product decay following a unit shutdown.

The RCS configuration for heat transport uses two RCS loops. Each RCS loop contains a SG and two reactor coolant pumps (RCPs). An RCP is located in each of the two SG cold legs. The pump flow rate has been sized to provide core heat removal with appropriate margin to departure from nucleate boiling (DNB) during power operation and for anticipated transients originating from power operation. This Specification requires two RCS loops with both RCPs in operation in each loop. The intent of the Specification is to require core heat removal with forced flow during power operation. Specifying two RCS loops provides the minimum necessary paths (two SGs) for heat removal.

APPLICABLE SAFETY ANALYSES

Safety analyses contain various assumptions for the Design Bases Accident (DBA) initial conditions including RCS pressure, RCS temperature, reactor power level, core parameters, and safety system setpoints. The important aspect for this LCO is the reactor coolant forced flow rate, which is represented by the number of RCS loops in service.

BASES

APPLICABLE SAFETY ANALYSES (continued)

Both transient and steady state analyses have been performed to establish the effect of flow on DNB. The transient or accident analysis for the plant has been performed assuming four RCPs are in operation. The majority of the plant safety analyses are based on initial conditions at high core power or zero power. The accident analyses that are of most importance to RCP operation are the four pump coastdown, single pump locked rotor, single pump (broken shaft or coastdown), and rod withdrawal events (Ref. 1).

Steady state DNB analysis had been performed for the [four] pump combination. For [four] pump operation, the steady state DNB analysis, which generates the pressure and temperature and Safety Limit (i.e., the departure from nucleate boiling ratio (DNBR) limit), assumes a maximum power level of 107% RTP. This is the design overpower condition for four pump operation. The 107% value is the accident analysis setpoint of the nuclear overpower (high flux) trip and is based on an analysis assumption that bounds possible instrumentation errors. The DNBR limit defines a locus of pressure and temperature points that result in a minimum DNBR greater than or equal to the critical heat flux correlation limit.

RCS Loops - MODES 1 and 2 satisfy Criteria 2 and 3 of 10 CFR 50.36(c)(2)(ii).

LCO

The purpose of this LCO is to require adequate forced flow for core heat removal. Flow is represented by having both RCS loops with both RCPs in each loop in operation for removal of heat by the two SGs. To meet safety analysis acceptance criteria for DNB, four pumps are required at rated power.

Each OPERABLE loop consists of two RCPs providing forced flow for heat transport to an SG that is OPERABLE. SG, and hence RCS loop, OPERABILITY with regard to SG water level is ensured by the Reactor Protection System (RPS) in MODES 1 and 2. A reactor trip places the plant in MODE 3 if any SG level is ≤ [25]% as sensed by the RPS. The minimum water level to declare the SG OPERABLE is [25]%.

APPLICABILITY

In MODES 1 and 2, the reactor is critical and thus has the potential to produce maximum THERMAL POWER. Thus, to ensure that the assumptions of the accident analyses remain valid, all RCS loops are required to be OPERABLE and in operation in these MODES to prevent DNB and core damage.

BASES

APPLICABILITY (continued)

The decay heat production rate is much lower than the full power heat rate. As such, the forced circulation flow and heat sink requirements are reduced for lower, noncritical MODES as indicated by the LCOs for MODES 3, 4, 5, and 6.

Operation in other MODES is covered by:

LCO 3.4.5, "RCS Loops - MODE 3,"
LCO 3.4.6, "RCS Loops - MODE 4,"
LCO 3.4.7, "RCS Loops - MODE 5, Loops Filled,"
LCO 3.4.8, "RCS Loops - MODE 5, Loops Not Filled,"
LCO 3.9.4, "Shutdown Cooling (SDC) and Coolant Circulation - High Water Level" (MODE 6), and
LCO 3.9.5, "Shutdown Cooling (SDC) and Coolant Circulation - Low Water Level" (MODE 6).

ACTIONS

A.1

If the requirements of the LCO are not met, the Required Action is to reduce power and bring the plant to MODE 3. This lowers power level and thus reduces the core heat removal needs and minimizes the possibility of violating DNB limits. It should be noted that the reactor will trip and place the plant in MODE 3 as soon as the RPS senses less than four RCPs operating.

The Completion Time of 6 hours is reasonable, based on operating experience, to reach MODE 3 from full power conditions in an orderly manner and without challenging safety systems.

SURVEILLANCE REQUIREMENTS

SR 3.4.4.1

This SR requires verification every 12 hours of the required number of loops in operation. Verification includes flow rate, temperature, or pump status monitoring, which help to ensure that forced flow is providing heat removal while maintaining the margin to DNB. The Frequency of 12 hours has been shown by operating practice to be sufficient to regularly assess degradation and verify operation within safety analyses assumptions. In addition, control room indication and alarms will normally indicate loop status.

REFERENCES

1. FSAR, Section [ ].

B 3.4 REACTOR COOLANT SYSTEM (RCS)

B 3.4.5 RCS Loops - MODE 3

BASES

BACKGROUND

The primary function of the reactor coolant in MODE 3 is removal of decay heat and transfer of this heat, via the steam generators (SGs), to the secondary plant fluid. The secondary function of the reactor coolant is to act as a carrier for soluble neutron poison, boric acid.

In MODE 3, reactor coolant pumps (RCPs) are used to provide forced circulation heat removal during heatup and cooldown. The MODE 3 decay heat removal requirements are low enough that a single RCS loop with one RCP is sufficient to remove core decay heat. However, [two] RCS loops are required to be OPERABLE to provide redundant paths for decay heat removal. Only one RCP needs to be OPERABLE to declare the associated RCS loop OPERABLE.

Reactor coolant natural circulation is not normally used but is sufficient for core cooling. However, natural circulation does not provide turbulent flow conditions. Therefore, boron reduction in natural circulation is prohibited because mixing to obtain a homogeneous concentration in all portions of the RCS cannot be ensured.

APPLICABLE SAFETY ANALYSES

Analyses have shown that the rod withdrawal event from MODE 3 with one RCS loop in operation is bounded by the rod withdrawal initiated from MODE 2.

Failure to provide heat removal may result in challenges to a fission product barrier. The RCS loops are part of the primary success path that functions or actuates to prevent or mitigate a Design Basis Accident or transient that either assumes the failure of, or presents a challenge to, the integrity of a fission product barrier.

RCS Loops - MODE 3 satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

The purpose of this LCO is to require both RCS loops to be available for heat removal, thus providing redundancy. The LCO requires both loops to be OPERABLE with the intent of requiring both SGs to be capable (> 25% water level) of transferring heat from the reactor coolant at a controlled rate. Forced reactor coolant flow is the required way to transport heat, although natural circulation flow provides adequate removal. A minimum of one running RCP meets the LCO requirement for one loop in operation.

BASES

LCO (continued)

The Note permits a limited period of operation without RCPs. All RCPs may be removed from operation for ≤ 1 hour per 8 hour period. This means that natural circulation has been established. When in natural circulation, a reduction in boron concentration with coolant at boron concentrations less than required to assure the SDM of LCO 3.1.1 is maintained is prohibited because an even concentration distribution throughout the RCS cannot be ensured. Core outlet temperature is to be maintained at least 10°F below the saturation temperature so that no vapor bubble may form and possibly cause a natural circulation flow obstruction.

In MODES 3, 4, and 5, it is sometimes necessary to stop all RCPs or shutdown cooling (SDC) pump forced circulation (e.g., to change operation from one SDC train to the other, to perform surveillance or startup testing, to perform the transition to and from SDC System cooling, or to avoid operation below the RCP minimum net positive suction head limit). The time period is acceptable because natural circulation is adequate for heat removal, or the reactor coolant temperature can be maintained subcooled and boron stratification affecting reactivity control is not expected.

An OPERABLE RCS loop consists of at least one OPERABLE RCP and an SG that is OPERABLE. A RCP is OPERABLE if it is capable of being powered and is able to provide forced flow if required.

APPLICABILITY

In MODE 3, the heat load is lower than at power; therefore, one RCS loop in operation is adequate for transport and heat removal. A second RCS loop is required to be OPERABLE but not in operation for redundant heat removal capability.

Operation in other MODES is covered by:

LCO 3.4.4,	"RCS Loops - MODES 1 and 2,"
LCO 3.4.6,	"RCS Loops - MODE 4,"
LCO 3.4.7,	"RCS Loops - MODE 5, Loops Filled,"
LCO 3.4.8,	"RCS Loops - MODE 5, Loops Not Filled,"
LCO 3.9.4,	"Shutdown Cooling (SDC) and Coolant Circulation - High Water Level" (MODE 6), and
LCO 3.9.5,	"Shutdown Cooling (SDC) and Coolant Circulation - Low Water Level" (MODE 6).

BASES

ACTIONS

A.1

If one RCS loop is inoperable, redundancy for forced flow heat removal is lost. The Required Action is restoration of the RCS loop to OPERABLE status within a Completion Time of 72 hours. This time allowance is a justified period to be without the redundant, nonoperating loop because a single loop in operation has a heat transfer capability greater than that needed to remove the decay heat produced in the reactor core.

B.1

If restoration for Required Action A.1 is not possible within 72 hours, the unit must be placed in MODE 4 within 12 hours. In MODE 4, the plant may be placed on the SDC System. The Completion Time of 12 hours is compatible with required operation to achieve cooldown and depressurization from the existing plant conditions in an orderly manner and without challenging plant systems.

C.1 and C.2

If two RCS loops are inoperable or a required RCS loop is not in operation, except as provided in Note 1 in the LCO section, all operations involving introduction of coolant into the RCS with boron concentration less than required to meet the minimum SDM of LCO 3.1.1 must be suspended. Action to restore one RCS loop to OPERABLE status and operation shall be initiated immediately and continued until one RCS loop is restored to OPERABLE status and operation. Suspending the introduction of coolant into the RCS of coolant with boron concentration less than required to meet the minimum SDM of LCO 3.1.1 is required to assure continued safe operation. With coolant added without forced circulation, unmixed coolant could be introduced to the core, however coolant added with boron concentration meeting the minimum SDM maintains acceptable margin to subcritical operation. The immediate Completion Times reflect the importance of maintaining operation for decay heat removal.

SURVEILLANCE REQUIREMENTS

SR 3.4.5.1

This SR requires verification every 12 hours that one RCS loop is in operation. Verification includes flow rate, temperature, and pump status monitoring, which help ensure that forced flow is providing heat removal. The 12 hour interval has been shown by operating practice to be sufficient to regularly assess degradation and verify operation within safety analyses assumptions. In addition, control room indication and alarms will normally indicate loop status.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.4.5.2

This SR requires verification every 12 hours that the secondary side water level in each SG is ≥ [25]%. An adequate SG water level is required in order to have a heat sink for removal of the core decay heat from the reactor coolant. The 12 hour interval has been shown by operating practice to be sufficient to regularly assess degradation and verify operation within the safety analyses assumptions.

SR 3.4.5.3

Verification that each required RCP is OPERABLE ensures that the single failure criterion is met and that an additional RCS loop can be placed in operation, if needed, to maintain decay heat removal and reactor coolant circulation. Verification is performed by verifying proper breaker alignment and power availability to each required RCP. Alternatively, verification that a pump is in operation also verifies proper breaker alignment and power availability. The Frequency of 7 days is considered reasonable in view of other administrative controls available and has been shown to be acceptable by operating experience.

This SR is modified by a Note that states the SR is not required to be performed until 24 hours after a required pump is not in operation.

REFERENCES None.

B 3.4 REACTOR COOLANT SYSTEM (RCS)

B 3.4.6 RCS Loops - MODE 4

BASES

BACKGROUND

In MODE 4, the primary function of the reactor coolant is the removal of decay heat and transfer of this heat to the steam generators (SGs) or shutdown cooling (SDC) heat exchangers. The secondary function of the reactor coolant is to act as a carrier for soluble neutron poison, boric acid.

In MODE 4, either reactor coolant pumps (RCPs) or SDC trains can be used for coolant circulation. The intent of this LCO is to provide forced flow from at least one RCP or one SDC train for decay heat removal and transport. The flow provided by one RCP loop or SDC train is adequate for heat removal. The other intent of this LCO is to require that two paths be available to provide redundancy for heat removal.

APPLICABLE SAFETY ANALYSES

In MODE 4, RCS circulation is considered in the determination of the time available for mitigation of the accidental boron dilution event. The RCS loops and SDC trains provide this circulation.

RCS Loops - MODE 4 satisfies Criterion 4 of 10 CFR 50.36(c)(2)(ii).

LCO

The purpose of this LCO is to require that at least two loops or trains, RCS or SDC, be OPERABLE in MODE 4 and one of these loops or trains be in operation. The LCO allows the two loops that are required to be OPERABLE to consist of any combination of RCS and SDC System loops. Any one loop or train in operation provides enough flow to remove the decay heat from the core with forced circulation. An additional loop or train is required to be OPERABLE to provide redundancy for heat removal.

Note 1 permits all RCPs and SDC pumps to be removed from operation ≤ 1 hour per 8 hour period. This means that natural circulation has been established using the SGs. The Note prohibits boron dilution with coolant at boron concentrations less than required to assure the SDM of LCO 3.1.1 is maintained when forced flow is stopped because an even concentration distribution cannot be ensured. Core outlet temperature is to be maintained at least 10°F below saturation temperature so that no vapor bubble may form and possibly cause a natural circulation flow obstruction. The response of the RCS without the RCPs or SDC pumps depends on the core decay heat load and the length of time that the

BASES

LCO (continued)

pumps are stopped. As decay heat diminishes, the effects on RCS temperature and pressure diminish. Without cooling by forced flow, higher heat loads will cause the reactor coolant temperature and pressure to increase at a rate proportional to the decay heat load. Because pressure can increase, the applicable system pressure limits (pressure and temperature (P/T) limits or low temperature overpressure protection (LTOP) limits) must be observed and forced SDC flow or heat removal via the SGs must be re-established prior to reaching the pressure limit. The circumstances for stopping both RCPs or SDC pumps are to be limited to situations where:

a. Pressure and temperature increases can be maintained well within the allowable pressure (P/T limits and LTOP) and 10°F subcooling limits or

b. An alternate heat removal path through the SGs is in operation.

Note 2 requires that either of the following two conditions be satisfied before an RCP may be started with any RCS cold leg temperature less than or equal to the LTOP enable temperature specified in the PTLR:

a. Pressurizer water level is < [60]% or

b. Secondary side water temperature in each SG is < [100]°F above each of the RCS cold leg temperatures.

Satisfying either of the above conditions will preclude a large pressure surge in the RCS when the RCP is started.

An OPERABLE RCS loop consists of at least one OPERABLE RCP and an SG that is OPERABLE and has the minimum water level specified in SR 3.4.6.2.

Similarly, for the SDC System, an OPERABLE SDC train is composed of the OPERABLE SDC pump(s) capable of providing forced flow to the SDC heat exchanger(s). RCPs and SDC pumps are OPERABLE if they are capable of being powered and are able to provide flow if required.

BASES

APPLICABILITY

In MODE 4, this LCO applies because it is possible to remove core decay heat and to provide proper boron mixing with either the RCS loops and SGs or the SDC System.

Operation in other MODES is covered by:

LCO 3.4.4,	"RCS Loops - MODES 1 and 2,"
LCO 3.4.5,	"RCS Loops - MODE 3,"
LCO 3.4.7,	"RCS Loops - MODE 5, Loops Filled,"
LCO 3.4.8,	"RCS Loops - MODE 5, Loops Not Filled,"
LCO 3.9.4,	"Shutdown Cooling and Coolant Circulation - High Water Level" (MODE 6), and
LCO 3.9.5,	"Shutdown Cooling and Coolant Circulation - Low Water Level" (MODE 6).

ACTIONS

A.1

If only one required RCS loop is OPERABLE and in operation and no SDC trains are OPERABLE, redundancy for heat removal is lost. Action must be initiated immediately to restore a required non-operating loop or train to OPERABLE status. The immediate Completion Time reflects the importance of maintaining the availability of two paths for decay heat removal.

A.2

If restoration is not accomplished and a SDC train is OPERABLE, the plant must be placed in MODE 5 within the next 24 hours. Placing the plant in MODE 5 is a conservative action with regard to decay heat removal. With only one SDC train OPERABLE, redundancy for decay heat removal is lost and, in the event of a loss of the remaining SDC train, it would be safer to initiate that loss from MODE 5 rather than MODE 4. The Completion Time of 24 hours is reasonable, based on operating experience, to reach MODE 5 from MODE 4, with only one SDC train operating, in an orderly manner and without challenging plant systems.

This Required Action is modified by a Note which indicates that the unit must be placed in MODE 5 only if a SDC train is OPERABLE. With no SDC train OPERABLE, the unit is in a condition with only limited cooldown capabilities. Therefore, the actions are to be concentrated on the restoration of a SDC train, rather than a cooldown of extended duration.

BASES

ACTIONS (continued)

B.1 and B.2

If two required loops or trains are inoperable or a required loop or train is not in operation except during conditions permitted by Note 1 in the LCO section, all operations involving introduction of coolant into the RCS with boron concentration less than required to meet the minimum SDM of LCO 3.1.1 must be suspended and action to restore one RCS loop or SDC train to OPERABLE status and operation must be initiated. The required margin to criticality must not be reduced in this type of operation. Suspending the introduction of coolant into the RCS of coolant with boron concentration less than required to meet the minimum SDM of LCO 3.1.1 is required to assure continued safe operation. With coolant added without forced circulation, unmixed coolant could be introduced to the core, however coolant added with boron concentration meeting the minimum SDM maintains acceptable margin to subcritical operations. The immediate Completion Times reflect the importance of decay heat removal. The action to restore must continue until one loop or train is restored to operation.

SURVEILLANCE REQUIREMENTS

SR 3.4.6.1

This SR requires verification every 12 hours that the required loop or train is in operation. This ensures forced flow is providing heat removal. Verification includes flow rate, temperature, or pump status monitoring. The 12 hour Frequency has been shown by operating practice to be sufficient to regularly assess RCS loop status. In addition, control room indication and alarms will normally indicate loop status.

SR 3.4.6.2

This SR requires verification every 12 hours of secondary side water level in the required SG(s) ≥ [25]%. An adequate SG water level is required in order to have a heat sink for removal of the core decay heat from the reactor coolant. The 12 hour interval has been shown by operating practice to be sufficient to regularly assess degradation and verify operation within safety analyses assumptions.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.4.6.3

Verification that each required pump is OPERABLE ensures that an additional RCS loop or SDC train can be placed in operation, if needed to maintain decay heat removal and reactor coolant circulation. Verification is performed by verifying proper breaker alignment and power available to each required pump. Alternatively, verification that a pump is in operation also verifies proper breaker alignment and power availability. The Frequency of 7 days is considered reasonable in view of other administrative controls available and has been shown to be acceptable by operating experience.

This SR is modified by a Note that states the SR is not required to be performed until 24 hours after a required pump is not in operation.

REFERENCES None.

B 3.4 REACTOR COOLANT SYSTEM (RCS)

B 3.4.7 RCS Loops - MODE 5, Loops Filled

BASES

BACKGROUND

In MODE 5 with the RCS loops filled, the primary function of the reactor coolant is the removal of decay heat and the transfer of this heat either to the steam generator (SG) secondary side coolant via natural circulation (Ref. 1) or the component cooling water via the shutdown cooling (SDC) heat exchangers. While the principal means for decay heat removal is via the SDC System, the SGs via natural circulation (Ref. 1) are specified as a backup means for redundancy. Even though the SGs cannot produce steam in this MODE, they are capable of being a heat sink due to their large contained volume of secondary side water. As long as the SG secondary side water is at a lower temperature than the reactor coolant, heat transfer will occur. The rate of heat transfer is directly proportional to the temperature difference. The secondary function of the reactor coolant is to act as a carrier for soluble neutron poison, boric acid.

In MODE 5 with RCS loops filled, the SDC trains are the principal means for decay heat removal. The number of trains in operation can vary to suit the operational needs. The intent of this LCO is to provide forced flow from at least one SDC train for decay heat removal and transport. The flow provided by one SDC train is adequate for decay heat removal. The other intent of this LCO is to require that a second path be available to provide redundancy for decay heat removal.

The LCO provides for redundant paths of decay heat removal capability. The first path can be an SDC train that must be OPERABLE and in operation. The second path can be another OPERABLE SDC train, or through the SGs via natural circulation (Ref. 1), each having an adequate water level.

APPLICABLE SAFETY ANALYSES

In MODE 5, RCS circulation is considered in the determination of the time available for mitigation of the accidental boron dilution event. The SDC trains provide this circulation.

RCS Loops - MODE 5 (Loops Filled) satisfies Criterion 4 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO

The purpose of this LCO is to require at least one of the SDC trains be OPERABLE and in operation with the other SDC train OPERABLE or secondary side water level of each SG shall be ≥ [25]%. One SDC train provides sufficient forced circulation to perform the safety functions of the reactor coolant under these conditions. The second SDC train is normally maintained OPERABLE as a backup to the operating SDC train to provide redundant paths for decay heat removal. However, if the standby SDC train is not OPERABLE, a sufficient alternate method to provide redundant paths for decay heat removal is two SGs with their secondary side water levels ≥ [25%]. Should the operating SDC train fail, the SGs could be used to remove the decay heat via natural circulation.

Note 1 permits all SDC pumps to be removed from operation ≤ 1 hour per 8 hour period. The circumstances for stopping both SDC trains are to be limited to situations where pressure and temperature increases can be maintained well within the allowable pressure (pressure and temperature and low temperature overpressure protection) and 10°F subcooling limits, or an alternate heat removal path through the SG(s) is in operation.

This LCO is modified by a Note that prohibits boron dilution with coolant at boron concentrations less than required to assure the SDM of LCO 3.1.1 is maintained when SDC forced flow is stopped because an even concentration distribution cannot be ensured. Core outlet temperature is to be maintained at least 10°F below saturation temperature, so that no vapor bubble would form and possibly cause a natural circulation flow obstruction. In this MODE, the SG(s) can be used as the backup for SDC heat removal. To ensure their availability, the RCS loop flow path is to be maintained with subcooled liquid.

In MODE 5, it is sometimes necessary to stop all RCP or SDC forced circulation. This is permitted to change operation from one SDC train to the other, perform surveillance or startup testing, perform the transition to and from the SDC, or to avoid operation below the RCP minimum net positive suction head limit. The time period is acceptable because natural circulation is acceptable for decay heat removal, the reactor coolant temperature can be maintained subcooled, and boron stratification affecting reactivity control is not expected.

Note 2 allows one SDC train to be inoperable for a period of up to 2 hours provided that the other SDC train is OPERABLE and in operation. This permits periodic surveillance tests to be performed on the inoperable train during the only time when such testing is safe and possible.

BASES

LCO (continued)

Note 3 requires that either of the following two conditions be satisfied before an RCP may be started with any RCS cold leg temperature less than or equal to the LTOP enable temperature specified in the PTLR:

a. Pressurizer water level must be < [60]% or

b. Secondary side water temperature in each SG must be < [100]°F above each of the RCS cold leg temperatures.

Satisfying either of the above conditions will preclude a low temperature overpressure event due to a thermal transient when the RCP is started.

Note 4 provides for an orderly transition from MODE 5 to MODE 4 during a planned heatup by permitting SDC trains to not be in operation when at least one RCP is in operation. This Note provides for the transition to MODE 4 where an RCP is permitted to be in operation and replaces the RCS circulation function provided by the SDC trains.

An OPERABLE SDC train is composed of an OPERABLE SDC pump and an OPERABLE SDC heat exchanger.

SDC pumps are OPERABLE if they are capable of being powered and are able to provide flow if required. A SG can perform as a heat sink via natural circulation when it has an adequate water level and is OPERABLE.

APPLICABILITY

In MODE 5 with RCS loops filled, this LCO requires forced circulation to remove decay heat from the core and to provide proper boron mixing. One SDC train provides sufficient circulation for these purposes.

Operation in other MODES is covered by:

LCO 3.4.4,	"RCS Loops - MODES 1 and 2,"
LCO 3.4.5,	"RCS Loops - MODE 3,"
LCO 3.4.6,	"RCS Loops – MODE 4,"
LCO 3.4.8,	"RCS Loops - MODE 5, Loops Not Filled,"
LCO 3.9.4,	"Shutdown Cooling (SDC) and Coolant Circulation - High Water Level" (MODE 6), and
LCO 3.9.5,	"Shutdown Cooling (SDC) and Coolant Circulation - Low Water Level" (MODE 6).

BASES

ACTIONS

A.1, A.2, B.1 and B.2

If one SDC train is OPERABLE and any required SGs has secondary side water levels < [25%], or one required SDC train is inoperable, redundancy for heat removal is lost. Action must be initiated immediately to restore a second SDC train to OPERABLE status or to restore the water level in the required SGs. Either Required Action will restore redundant decay heat removal paths. The immediate Completion Times reflect the importance of maintaining the availability of two paths for decay heat removal.

C.1 and C.2

If a required SDC train is not in operation, or no required SDC train is OPERABLE, except as permitted in Note 1, all operations involving introduction of coolant into the RCS with boron concentration less than required to meet the minimum SDM of LCO 3.1.1 must be suspended. Action to restore one SDC train to OPERABLE status and operation must be initiated. The required margin to criticality must not be reduced in this type of operation. Suspending the introduction of coolant into the RCS of coolant with boron concentration less than required to meet the minimum SDM of LCO 3.1.1 is required to assure continued safe operation. With coolant added without forced circulation, unmixed coolant could be introduced to the core, however coolant added with boron concentration meeting the minimum SDM maintains acceptable margin to subcritical operations. The immediate Completion Times reflect the importance of maintaining operation for decay heat removal.

SURVEILLANCE REQUIREMENTS

SR 3.4.7.1

This SR requires verification every 12 hours that one SDC train is in operation. Verification includes flow rate, temperature, or pump status monitoring, which help ensure that forced flow is providing decay heat removal. The 12 hour Frequency has been shown by operating practice to be sufficient to regularly assess degradation and verify operation is within safety analyses assumptions. In addition, control room indication and alarms will normally indicate loop status.

The SDC flow is established to ensure that core outlet temperature is maintained sufficiently below saturation to allow time for swapover to the standby SDC train should the operating train be lost.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.4.7.2

Verifying the SGs are OPERABLE by ensuring their secondary side water levels are ≥ [25%] ensures that redundant heat removal paths are available if the second SDC train is inoperable. The Surveillance is required to be performed when the LCO requirement is being met by use of the SGs. If both SDC trains are OPERABLE, this SR is not needed. The 12 hour Frequency has been shown by operating practice to be sufficient to regularly assess degradation and verify operation within safety analyses assumptions.

SR 3.4.7.3

Verification that each required SDC train is OPERABLE ensures that redundant paths for decay heat removal are available. The requirement also ensures that the additional train can be placed in operation, if needed, to maintain decay heat removal and reactor coolant circulation. Verification is performed by verifying proper breaker alignment and power available to each required pump. Alternatively, verification that a pump is in operation also verifies proper breaker alignment and power availability. The Surveillance is required to be performed when the LCO requirement is being met by one of two SDC trains, e.g., both SGs have < [25]% water level. The Frequency of 7 days is considered reasonable in view of other administrative controls available and has been shown to be acceptable by operating experience.

This SR is modified by a Note that states the SR is not required to be performed until 24 hours after a required pump is not in operation.

REFERENCES

1. NRC Information Notice 95-35, "Degraded Ability of Steam Generators to Remove Decay Heat by Natural Circulation."

B 3.4 REACTOR COOLANT SYSTEM (RCS)

B 3.4.8 RCS Loops - MODE 5, Loops Not Filled

BASES

BACKGROUND

In MODE 5 with the RCS loops not filled, the primary function of the reactor coolant is the removal of decay heat and transfer of this heat to the shutdown cooling (SDC) heat exchangers. The steam generators (SGs) are not available as a heat sink when the loops are not filled. The secondary function of the reactor coolant is to act as a carrier for the soluble neutron poison, boric acid.

In MODE 5 with loops not filled, only the SDC System can be used for coolant circulation. The number of trains in operation can vary to suit the operational needs. The intent of this LCO is to provide forced flow from at least one SDC train for decay heat removal and transport and to require that two paths be available to provide redundancy for heat removal.

APPLICABLE SAFETY ANALYSES

In MODE 5, RCS circulation is considered in determining the time available for mitigation of the accidental boron dilution event. The SDC trains provide this circulation. The flow provided by one SDC train is adequate for decay heat removal and for boron mixing.

RCS loops - MODE 5 (loops not filled) satisfies Criterion 4 of 10 CFR 50.36(c)(2)(ii).

LCO

The purpose of this LCO is to require a minimum of two SDC trains be OPERABLE and one of these trains be in operation. An OPERABLE train is one that is capable of transferring heat from the reactor coolant at a controlled rate. Heat cannot be removed via the SDC System unless forced flow is used. A minimum of one running SDC pump meets the LCO requirement for one train in operation. An additional SDC train is required to be OPERABLE to meet the single failure criterion.

Note 1 permits the SDC pumps to be removed from operation for ≤ 15 minutes when switching from one train to another. The circumstances for stopping both SDC pumps are to be limited to situations when the outage time is short [and the core outlet temperature is maintained > 10°F below saturation temperature]. The Note prohibits boron dilution with coolant at boron concentrations less than required to assure the SDM of LCO 3.1.1 is maintained or draining operations when SDC forced flow is stopped.

Note 2 allows one SDC train to be inoperable for a period of 2 hours provided that the other train is OPERABLE and in operation. This permits periodic surveillance tests to be performed on the inoperable train during the only time when these tests are safe and possible.

BASES

LCO (continued)

An OPERABLE SDC train is composed of an OPERABLE SDC pump capable of providing forced flow to an OPERABLE SDC heat exchanger, along with the appropriate flow and temperature instrumentation for control, protection, and indication. SDC pumps are OPERABLE if they are capable of being powered and are able to provide flow if required.

APPLICABILITY

In MODE 5 with loops not filled, this LCO requires core heat removal and coolant circulation by the SDC System.

Operation in other MODES is covered by:

LCO 3.4.4,	"RCS Loops - MODES 1 and 2,"
LCO 3.4.5,	"RCS Loops - MODE 3,"
LCO 3.4.6,	"RCS Loops - MODE 4,"
LCO 3.4.7,	"RCS Loops - MODE 5, Loops Filled,"
LCO 3.9.4,	"Shutdown Cooling (SDC) and Coolant Circulation - High Water Level" (MODE 6), and
LCO 3.9.5,	"Shutdown Cooling (SDC) and Coolant Circulation - Low Water Level" (MODE 6).

ACTIONS

A.1

If one required SDC train is inoperable, redundancy for heat removal is lost. Action must be initiated immediately to restore a second train to OPERABLE status. The Completion Time reflects the importance of maintaining the availability of two paths for heat removal.

B.1 and B.2

If no required SDC train is OPERABLE or the required train is not in operation, except as provided in Note 1, all operations involving introduction of coolant into the RCS with boron concentration less than required to meet the minimum SDM of LCO 3.1.1 must be suspended. Action to restore one SDC train to OPERABLE status and operation must be initiated immediately. The required margin to criticality must not be reduced in this type of operation. Suspending the introduction of coolant into the RCS of coolant with boron concentration less than required to meet the minimum SDM of LCO 3.1.1 is required to assure continued safe operation. With coolant added without forced circulation, unmixed coolant could be introduced to the core, however coolant added with boron concentration meeting the minimum SDM maintains acceptable margin to subcritical operations. The immediate Completion Time reflects the importance of maintaining operation for decay heat removal.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.4.8.1

This SR requires verification every 12 hours that the required SDC train is in operation. Verification includes flow rate, temperature, or pump status monitoring, which help ensure that forced flow is providing decay heat removal. The 12 hour Frequency has been shown by operating practice to be sufficient to regularly assess degradation and verify operation is within safety analyses assumptions.

SR 3.4.8.2

Verification that each required train is OPERABLE ensures that redundant paths for heat removal are available and that an additional train can be placed in operation, if needed, to maintain decay heat removal and reactor coolant circulation. Verification is performed by verifying proper breaker alignment and indicated power available to each required pump. Alternatively, verification that a pump is in operation also verifies proper breaker alignment and power availability. The Frequency of 7 days is considered reasonable in view of other administrative controls available and has been shown to be acceptable by operating experience.

This SR is modified by a Note that states the SR is not required to be performed until 24 hours after a required pump is not in operation.

REFERENCES

None.

B 3.4 REACTOR COOLANT SYSTEM (RCS)

B 3.4.9 Pressurizer

BASES

BACKGROUND

The pressurizer provides a point in the RCS where liquid and vapor are maintained in equilibrium under saturated conditions for pressure control purposes to prevent bulk boiling in the remainder of the RCS. Key functions include maintaining required primary system pressure during steady state operation and limiting the pressure changes caused by reactor coolant thermal expansion and contraction during normal load transients.

The pressure control components addressed by this LCO include the pressurizer water level, the required heaters and their backup heater controls, and emergency power supplies. Pressurizer safety valves and pressurizer power operated relief valves (PORVs) are addressed by LCO 3.4.10, "Pressurizer Safety Valves," and LCO 3.4.11, "Pressurizer Power Operated Relief Valves (PORVs)," respectively.

The maximum water level limit has been established to ensure that a liquid to vapor interface exists to permit RCS pressure control, using the sprays and heaters during normal operation and proper pressure response for anticipated design basis transients. The water level limit serves two purposes:

a. Pressure control during normal operation maintains subcooled reactor coolant in the loops and thus in the preferred state for heat transport and

b. By restricting the level to a maximum, expected transient reactor coolant volume increases (pressurizer insurge) will not cause excessive level changes that could result in degraded ability for pressure control.

The maximum water level limit permits pressure control equipment to function as designed. The limit preserves the steam space during normal operation, thus, both sprays and heaters can operate to maintain the design operating pressure. The level limit also prevents filling the pressurizer (water solid) for anticipated design basis transients, thus ensuring that pressure relief devices (PORVs or pressurizer safety valves) can control pressure by steam relief rather than water relief. If the level limits were exceeded prior to a transient that creates a large pressurizer insurge volume leading to water relief, the maximum RCS pressure might exceed the Safety Limit of 2750 psig.

BASES

BACKGROUND (continued)

The requirement to have [two groups of] pressurizer heaters ensures that RCS pressure can be maintained. The pressurizer heaters maintain RCS pressure to keep the reactor coolant subcooled. Inability to control RCS pressure during natural circulation flow could result in loss of single phase flow and decreased capability to remove core decay heat.

APPLICABLE SAFETY ANALYSES

In MODES 1, 2, and 3, the LCO requirement for a steam bubble is reflected implicitly in the accident analyses. No safety analyses are performed in lower MODES. All analyses performed from a critical reactor condition assume the existence of a steam bubble and saturated conditions in the pressurizer. In making this assumption, the analyses neglect the small fraction of noncondensible gases normally present.

Safety analyses presented in the FSAR do not take credit for pressurizer heater operation; however, an implicit initial condition assumption of the safety analyses is that the RCS is operating at normal pressure.

Although the heaters are not specifically used in accident analysis, the need to maintain subcooling in the long term during loss of offsite power, as indicated in NUREG-0737 (Ref. 1), is the reason for their inclusion. The requirement for emergency power supplies is based on NUREG-0737 (Ref. 1). The intent is to keep the reactor coolant in a subcooled condition with natural circulation at hot, high pressure conditions for an undefined, but extended, time period after a loss of offsite power. While loss of offsite power is a coincident occurrence assumed in the accident analyses, maintaining hot, high pressure conditions over an extended time period is not evaluated in the accident analyses.

The pressurizer satisfies Criterion 2 and Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

-----------------------------------REVIEWER'S NOTE-----------------------------------
Plants licensed prior to the issuance of NUREG-0737 may not have a requirement on the number of pressurizer groups.

The LCO requirement for the pressurizer to be OPERABLE with water level < [60]% ensures that a steam bubble exists. Limiting the maximum operating water level preserves the steam space for pressure control. The LCO has been established to minimize the consequences of potential overpressure transients. Requiring the presence of a steam bubble is also consistent with analytical assumptions.

BASES

LCO (continued)

The LCO requires [two groups of] OPERABLE pressurizer heaters, [each] with a capacity ≥ [150] kW [and capable of being powered from an emergency power supply]. The minimum heater capacity required is sufficient to maintain the RCS near normal operating pressure when accounting for heat losses through the pressurizer insulation. By maintaining the pressure near the operating conditions, a wide subcooling margin to saturation can be obtained in the loops. The exact design value of [150] kW is derived from the use of 12 heaters rated at 12.5 kW each. The amount needed to maintain pressure is dependent on the ambient heat losses.

APPLICABILITY

The need for pressure control is most pertinent when core heat can cause the greatest effect on RCS temperature resulting in the greatest effect on pressurizer level and RCS pressure control. Thus, Applicability has been designated for MODES 1 and 2. The Applicability is also provided for MODE 3. The purpose is to prevent solid water RCS operation during heatup and cooldown to avoid rapid pressure rises caused by normal operational perturbation, such as reactor coolant pump startup. The LCO does not apply to MODE 5 (Loops Filled) because LCO 3.4.12, "Low Temperature Overpressure Protection (LTOP) System," applies. The LCO does not apply to MODES 5 and 6 with partial loop operation.

In MODES 1, 2, and 3, there is the need to maintain the availability of pressurizer heaters capable of being powered from an emergency power supply. In the event of a loss of offsite power, the initial conditions of these MODES gives the greatest demand for maintaining the RCS in a hot pressurized condition with loop subcooling for an extended period. For MODE 4, 5, or 6, it is not necessary to control pressure (by heaters) to ensure loop subcooling for heat transfer when the Shutdown Cooling System is in service and therefore the LCO is not applicable.

ACTIONS

A.1 and A.2

With pressurizer water level not within the limit, action must be taken to restore the plant to operation within the bounds of the safety analyses. To achieve this status, the unit must be brought to MODE 3, with the reactor trip breakers open, within 6 hours and to MODE 4 within [12] hours. This takes the plant out of the applicable MODES and restores the plant to operation within the bounds of the safety analyses.

BASES

ACTIONS (continued)

Six hours is reasonable, based on operating experience, to reach MODE 3 from full power in an orderly manner and without challenging plant systems. Further pressure and temperature reduction to MODE 4 brings the plant to a MODE where the LCO is not applicable. The 12 hour time to reach the nonapplicable MODE is reasonable based on operating experience for that evolution.

B.1

If one [required] group of pressurizer heaters is inoperable, restoration is required within 72 hours. The Completion Time of 72 hours is reasonable considering that a demand caused by loss of offsite power would be unlikely in this period. Pressure control may be maintained during this time using normal station powered heaters.

C.1 and C.2

If one [required] group of pressurizer heaters is inoperable and cannot be restored within the allowed Completion Time of Required Action B.1, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to MODE 3 within 6 hours and to MODE 4 within [12] hours. The Completion Time of 6 hours is reasonable, based on operating experience, to reach MODE 3 from full power in an orderly manner and without challenging safety systems. Similarly, the Completion Time of [12] hours is reasonable, based on operating experience, to reach MODE 4 from full power in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.4.9.1

This Surveillance ensures that during steady state operation, pressurizer water level is maintained below the nominal upper limit to provide a minimum space for a steam bubble. The Surveillance is performed by observing the indicated level. The 12 hour interval has been shown by operating practice to be sufficient to regularly assess the level for any deviation and verify that operation is within safety analyses assumptions. Alarms are also available for early detection of abnormal level indications.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.4.9.2

-----------------------------------REVIEWER'S NOTE-----------------------------------
The frequency for performing pressurizer heater capacity testing shall be either 18 months or 92 days, depending on whether or not the plant has dedicated safety-related heaters. For dedicated safety-related heaters, which do not normally operate, 92 days is applied. For non-dedicated safety-related heaters, which normally operate, 18 months is applied.

The Surveillance is satisfied when the power supplies are demonstrated to be capable of producing the minimum power and the associated pressurizer heaters are verified to be at their design rating. (This may be done by testing the power supply output and by performing an electrical check on heater element continuity and resistance.) The Frequency of [18] months is considered adequate to detect heater degradation and has been shown by operating experience to be acceptable.

[SR 3.4.9.3

This SR is not applicable if the heaters are permanently powered by 1E power supplies.

This Surveillance demonstrates that the heaters can be manually transferred to and energized by emergency power supplies. The Frequency of [18] months is based on a typical fuel cycle and industry accepted practice. This is consistent with similar verifications of emergency power.]

REFERENCES

1. NUREG-0737, November 1980.

B 3.4 REACTOR COOLANT SYSTEM (RCS)

B 3.4.10 Pressurizer Safety Valves

BASES

BACKGROUND

The purpose of the two spring loaded pressurizer safety valves is to provide RCS overpressure protection. Operating in conjunction with the Reactor Protection System, two valves are used to ensure that the Safety Limit (SL) of 2750 psia is not exceeded for analyzed transients during operation in MODES 1 and 2. Two safety valves are used for MODE 3 and portions of MODE 4. For the remainder of MODE 4, MODE 5, and MODE 6 with the head on, overpressure protection is provided by operating procedures and the LCO 3.4.12, "Low Temperature Overpressure Protection (LTOP) System."

The self actuated pressurizer safety valves are designed in accordance with the requirements set forth in the ASME, Boiler and Pressure Vessel Code, Section III (Ref. 1). The required lift pressure is 2500 psia ± 1%. The safety valves discharge steam from the pressurizer to a quench tank located in the containment. The discharge flow is indicated by an increase in temperature downstream of the safety valves and by an increase in the quench tank temperature and level.

The upper and lower pressure limits are based on the ± 1%-tolerance requirement (Ref. 1) for lifting pressures above 1000 psig. The lift setting is for the ambient conditions associated with MODES 1, 2, and 3. This requires either that the valves be set hot or that a correlation between hot and cold settings be established.

The pressurizer safety valves are part of the primary success path and mitigate the effects of postulated accidents. OPERABILITY of the safety valves ensures that the RCS pressure will be limited to 110% of design pressure. The consequences of exceeding the ASME pressure limit (Ref. 1) could include damage to RCS components, increased leakage, or a requirement to perform additional stress analyses prior to resumption of reactor operation.

APPLICABLE SAFETY ANALYSES

All accident analyses in the FSAR that require safety valve actuation assume operation of both pressurizer safety valves to limit increasing reactor coolant pressure. The overpressure protection analysis is also based on operation of both safety valves and assumes that the valves open at the high range of the setting (2500-psia system design pressure plus 1%). These valves must accommodate pressurizer insurges that

BASES

APPLICABLE SAFETY ANALYSES (continued)

could occur during a startup, rod withdrawal, ejected rod, loss of main feedwater, or main feedwater line break accident. The startup accident establishes the minimum safety valve capacity. The startup accident is assumed to occur at < 15% power. Single failure of a safety valve is neither assumed in the accident analysis nor required to be addressed by the ASME Code. Compliance with this specification is required to ensure that the accident analysis and design basis calculations remain valid.

The pressurizer safety valves satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

The [two] pressurizer safety valves are set to open at the RCS design pressure (2500 psia) and within the ASME specified tolerance to avoid exceeding the maximum RCS design pressure SL, to maintain accident analysis assumptions, and to comply with ASME Code requirements. The upper and lower pressure tolerance limits are based on the ± 1% tolerance requirements (Ref. 1) for lifting pressures above 1000 psig. The limit protected by this specification is the reactor coolant pressure boundary (RCPB) SL of 110% of design pressure. Inoperability of one or both valves could result in exceeding the SL if a transient were to occur. The consequences of exceeding the ASME pressure limit could include damage to one or more RCS components, increased leakage, or additional stress analysis being required prior to resumption of reactor operation.

APPLICABILITY

In MODES 1, 2, and 3, and portions of MODE 4 above the LTOP temperature, OPERABILITY of [two] valves is required because the combined capacity is required to keep reactor coolant pressure below 110% of its design value during certain accidents. MODE 3 and portions of MODE 4 are conservatively included, although the listed accidents may not require both safety valves for protection.

The LCO is not applicable in MODE 4 when any RCS cold leg temperature is less than or equal to the LTOP enable temperature specified in the PTLR and MODE 5 because LTOP protection is provided. Overpressure protection is not required in MODE 6 with the reactor vessel head detensioned.

The Note allows entry into MODES 3 and 4 with the lift settings outside the LCO limits. This permits testing and examination of the safety valves at high pressure and temperature near their normal operating range, but only after the valves have had a preliminary cold setting. The cold setting gives assurance that the valves are OPERABLE near their design condition. Only one valve at a time will be removed from service for testing. The [36] hour exception is based on 18 hour outage time for each of the two valves. The 18 hour period is derived from operating experience that hot testing can be performed within this timeframe.

BASES

ACTIONS

A.1

With one pressurizer safety valve inoperable, restoration must take place within 15 minutes. The Completion Time of 15 minutes reflects the importance of maintaining the RCS overpressure protection system. An inoperable safety valve coincident with an RCS overpressure event could challenge the integrity of the RCPB.

B.1 and B.2

If the Required Action cannot be met within the required Completion Time or if two or more pressurizer safety valves are inoperable, the plant must be brought to a MODE in which the requirement does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 4 with any RCS cold leg temperature less than or equal to the LTOP enable temperature specified in the PTLR within [24] hours. The 6 hours allowed is reasonable, based on operating experience, to reach MODE 3 from full power without challenging plant systems. Similarly, the [24] hours allowed is reasonable, based on operating experience, to reach MODE 4 without challenging plant systems. With any RCS cold leg temperature less than or equal to the LTOP enable temperature specified in the PTLR, overpressure protection is provided by LTOP. The change from MODE 1, 2, or 3 to MODE 4 reduces the RCS energy (core power and pressure), lowers the potential for large pressurizer insurges, and thereby removes the need for overpressure protection by [two] pressurizer safety valves.

SURVEILLANCE REQUIREMENTS

SR 3.4.10.1

SRs are specified in the Inservice Testing Program. Pressurizer safety valves are to be tested in accordance with the requirements of the ASME Code (Ref. 1), which provides the activities and the Frequency necessary to satisfy the SRs. No additional requirements are specified.

The pressurizer safety valve setpoint is ± [3]% for OPERABILITY; however, the valves are reset to ± 1% during the Surveillance to allow for drift.

REFERENCES

1. ASME Code for Operation and Maintenance of Nuclear Power Plants.

B 3.4 REACTOR COOLANT SYSTEM (RCS)

B 3.4.11 Pressurizer Power Operated Relief Valves (PORVs)

BASES

BACKGROUND

The pressurizer is equipped with two types of devices for pressure relief: pressurizer safety valves and PORVs. The PORV is an air operated valve that is automatically opened at a specific set pressure when the pressurizer pressure increases and is automatically closed on decreasing pressure. The PORV may also be manually operated using controls installed in the control room.

An electric, motor operated, normally open, block valve is installed between the pressurizer and the PORV. The function of the block valve is to isolate the PORV. Block valve closure is accomplished manually using controls in the control room and may be used to isolate a leaking PORV to permit continued power operation. Most importantly, the block valve is used to isolate a stuck open PORV to isolate the resulting small break loss of coolant accident (LOCA). Closure terminates the RCS depressurization and coolant inventory loss.

The PORV and its block valve controls are powered from normal power supplies. Their controls are also capable of being powered from emergency supplies. Power supplies for the PORV are separate from those for the block valve. Power supply requirements are defined in NUREG-0737, Paragraph II, G.1 (Ref. 1).

The PORV setpoint is above the high pressure reactor trip setpoint and below the opening setpoint for the pressurizer safety valves as required by Reference 2. The purpose of the relationship of these setpoints is to limit the number of transient pressure increase challenges that might open the PORV, which, if opened, could fail in the open position. The PORV setpoint thus limits the frequency of challenges from transients and limits the possibility of a small break LOCA from a failed open PORV. Placing the setpoint below the pressurizer safety valve opening setpoint reduces the frequency of challenges to the safety valves, which, unlike the PORV, cannot be isolated if they were to fail to open.

The primary purpose of this LCO is to ensure that the PORV and the block valve are operating correctly so the potential for a small break LOCA through the PORV pathway is minimized, or if a small break LOCA were to occur through a failed open PORV, the block valve could be manually operated to isolate the path.

BASES

BACKGROUND (continued)

The PORV may be manually operated to depressurize the RCS as deemed necessary by the operator in response to normal or abnormal transients. The PORV may be used for depressurization when the pressurizer spray is not available, a condition that may be encountered during loss of offsite power. Operators can manually open the PORVs to reduce RCS pressure in the event of a steam generator tube rupture (SGTR) with offsite power unavailable.

The PORV may also be used for feed and bleed core cooling in the case of multiple equipment failure events that are not within the design basis, such as a total loss of feedwater.

The PORV functions as an automatic overpressure device and limits challenges to the safety valves. Although the PORV acts as an overpressure device for operational purposes, safety analyses [do not take credit for PORV actuation, but] do take credit for the safety valves.

The PORV also provides low temperature overpressure protection (LTOP) during heatup and cooldown. LCO 3.4.12, "Low Temperature Overpressure Protection (LTOP) System," addresses this function.

APPLICABLE SAFETY ANALYSES

The PORV small break LOCA break size is bounded by the spectrum of piping breaks analyzed for plant licensing. Because the PORV small break LOCA is located at the top of the pressurizer, the RCS response characteristics are different from RCS loop piping breaks; analyses have been performed to investigate these characteristics.

The possibility of a small break LOCA through the PORV is reduced when the PORV flow path is OPERABLE and the PORV opening setpoint is established to be reasonably remote from expected transient challenges. The possibility is minimized if the flow path is isolated.

The PORV opening setpoint has been established in accordance with Reference 2. It has been set so expected RCS pressure increases from anticipated transients will not challenge the PORV, minimizing the possibility of small break LOCA through the PORV.

Overpressure protection is provided by safety valves, and analyses do not take credit for the PORV opening for accident mitigation.

Pressurizer PORVs satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO

The LCO requires the PORV and its associated block valve to be OPERABLE. The block valve is required to be OPERABLE so it may be used to isolate the flow path if the PORV is not OPERABLE.

Valve OPERABILITY also means the PORV setpoint is correct. By ensuring that the PORV opening setpoint is correct, the PORV is not subject to frequent challenges from possible pressure increase transients, and therefore the possibility of a small break LOCA through a failed open PORV is not a frequent event.

APPLICABILITY

In MODES 1, 2, and 3, the PORV and its block valve are required to be OPERABLE to limit the potential for a small break LOCA through the flow path. A likely cause for PORV small break LOCA is a result of pressure increase transients that cause the PORV to open. Imbalances in the energy output of the core and heat removal by the secondary system can cause the RCS pressure to increase to the PORV opening setpoint. Pressure increase transients can occur any time the steam generators are used for heat removal. The most rapid increases will occur at higher operating power and pressure conditions of MODES 1 and 2.

Pressure increases are less prominent in MODE 3 because the core input energy is reduced, but the RCS pressure is high. Therefore, this LCO is applicable in MODES 1, 2, and 3. The LCO is not applicable in MODE 4 when both pressure and core energy are decreased and the pressure surges become much less significant. The PORV setpoint is reduced for LTOP in MODES 4, 5, and 6 with the reactor vessel head in place. LCO 3.4.12 addresses the PORV requirements in these MODES.

ACTIONS

The ACTIONS are modified by a Note. The Note clarifies that all pressurizer PORVs and block valves are treated as separate entities, each with separate Completion Times (i.e., the Completion Time is on a component basis).

A.1

With the PORV inoperable and capable of being manually cycled, either the PORV must be restored or the flow path isolated within 1 hour. The block valve should be closed but power must be maintained to the associated block valve, since removal of power would render the block valve inoperable. Although the PORV may be designated inoperable, it may be able to be manually opened and closed and in this manner can be used to perform its function. PORV inoperability may be due to seat leakage, instrumentation problems, automatic control problems, or other causes that do not prevent manual use and do not create a possibility for

BASES

ACTIONS (continued)

a small break LOCA. For these reasons, the block valve may be closed but the Action requires power be maintained to the valve. This Condition is only intended to permit operation of the plant for a limited period of time not to exceed the next refueling outage (MODE 6) so that maintenance can be performed on the PORVs to eliminate the problem condition. The PORVs should normally be available for automatic mitigation of overpressure events and should be returned to OPERABLE status prior to entering startup (MODE 2).

Quick access to the PORV for pressure control can be made when power remains on the closed block valve. The Completion Time of 1 hour is based on plant operating experience that minor problems can be corrected or closure can be accomplished in this time period.

<u>B.1, B.2, and B.3</u>

If one PORV is inoperable and not capable of being manually cycled, it must either be isolated, by closing the associated block valve and removing the power from the block valve, or restored to OPERABLE status. The Completion Time of 1 hour is reasonable, based on challenges to the PORVs during this time period, and provides the operator adequate time to correct the situation. If the inoperable valve cannot be restored to OPERABLE status, it must be isolated within the specified time. Because there is at least one PORV that remains OPERABLE, an additional 72 hours is provided to restore the inoperable PORV to OPERABLE status.

<u>C.1 and C.2</u>

If one block valve is inoperable, then it must be restored to OPERABLE status, or the associated PORV placed in manual control. The prime importance for the capability to close the block valve is to isolate a stuck open PORV. Therefore, if the block valve cannot be restored to OPERABLE status within 1 hour, the Required Action is to place the PORV in manual control to preclude its automatic opening for an overpressure event and to avoid the potential for a stuck open PORV at a time that the block valve is inoperable. The Completion Times of 1 hour are reasonable based on the small potential for challenges to the system during this time period and provide the operator time to correct the situation. Because at least one PORV remains OPERABLE, the operator is permitted a Completion Time of 72 hours to restore the inoperable block valve to OPERABLE status. The time allowed to restore the block

BASES

ACTIONS (continued)

valve is based upon the Completion Time for restoring an inoperable PORV in Condition B since the PORVs are not capable of automatically mitigating an overpressure event when placed in manual control. If the block valve is restored within the Completion Time of 72 hours, the power will be restored and the PORV restored to OPERABLE status.

D.1 and D.2

If the Required Action cannot be met within the associated Completion Time, the plant must be brought to a MODE in which the requirement does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 4 within 12 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

E.1, E.2, E.3, and E.4

If more than one PORV is inoperable and not capable of being manually cycled, it is necessary to either restore at least one valve within the Completion Time of 1 hour or isolate the flow path by closing and removing the power to the associated block valves. The Completion Time of 1 hour is reasonable based on the small potential for challenges to the system during this time and provides the operator time to correct the situation. If one PORV is restored and one PORV remains inoperable, then the plant will be in Condition B with the time clock started at the original declaration of having two PORVs inoperable. If no PORVs are restored within the Completion Time, then the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 4 within 12 hours. The Completion Time of 6 hours is reasonable, based on operating experience, to reach MODE 3 from full power in an orderly manner and without challenging plant systems. Similarly, the Completion Time of 12 hours to reach MODE 4 is reasonable, considering that a plant can cool down within that time frame on one safety system train. In MODES 4 and 5, maintaining PORV OPERABILITY may be required. See LCO 3.4.12.

BASES

ACTIONS (continued)

F.1

If two block valves are inoperable, it is necessary to restore at least one block valve to OPERABLE status within 2 hours. The Completion Time is reasonable based on the small potential for challenges to the system during this time and provides the operator time to correct the situation.

G.1 and G.2

If the Required Actions and associated Completion Times of Condition E or F are not met, then the plant must be brought to a MODE in which the LCO does not apply. The plant must be brought to at least MODE 3 within 6 hours and to MODE 4 within 12 hours. The Completion Time of 6 hours is reasonable, based on operating experience, to reach MODE 3 from full power in an orderly manner and without challenging safety systems. Similarly, the Completion Time of 12 hours to reach MODE 4 is reasonable considering that a plant can cool down within that time frame on one safety system train. In MODES 4 and 5, maintaining PORV OPERABILITY may be required. See LCO 3.4.12.

SURVEILLANCE REQUIREMENTS

SR 3.4.11.1

Block valve cycling verifies that it can be closed if necessary. The basis for the Frequency of [92 days] is the ASME Code (Ref. 3).

This SR is modified by two Notes. Note 1 modifies this SR by stating that this SR is not required to be performed with the block valve closed in accordance with the Required Actions of this LCO. Opening the block valve in this condition increases the risk of an unisolable leak from the RCS since the PORV is already inoperable. Note 2 modifies this SR to allow entry into and operation in MODE 3 prior to performing the SR. This allows the test to be performed in MODE 3 under operating temperature and pressure conditions, prior to entering MODE 1 or 2. [In accordance with Reference 4, administrative controls require this test be performed in MODE 3 or 4 to adequately simulate operating temperature and pressure effects on PORV operation.]

SR 3.4.11.2

SR 3.4.11.2 requires complete cycling of each PORV. PORV cycling demonstrates its function. The Frequency of [18] months is based on a typical refueling cycle and industry accepted practice.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The Note modifies this SR to allow entry into and operation in MODE 3 prior to performing the SR. This allows the test to be performed in MODE 3 under operating temperature and pressure conditions, prior to entering MODE 1 or 2. [In accordance with Reference 4, administrative controls require this test be performed in MODE 3 or 4 to adequately simulate operating temperature and pressure effects on PORV operation.]

[SR 3.4.11.3

Operating the solenoid air control valves and check valves on the air accumulators ensures the PORV control system actuates properly when called upon. The Frequency of [18] months is based on a typical refueling cycle and the Frequency of the other surveillances used to demonstrate PORV OPERABILITY.]

[SR 3.4.11.4

This Surveillance is not required for plants with permanent 1E power supplies to the valves. The test demonstrates that emergency power can be provided and is performed by transferring power from the normal supply to the emergency supply and cycling the valves. The Frequency of [18] months is based on a typical refueling cycle and industry accepted practice.]

REFERENCES

1. NUREG-0737, Paragraph II, G.I, November 1980.

2. Inspection and Enforcement (IE) Bulletin 79-05B, April 21, 1979.

3. ASME Code for Operation and Maintenance of Nuclear Power Plants.

[4. Generic Letter 90-06, "Resolution of Generic Issue 70, 'Power-Operated Relief Valve and Block Valve Reliability,' and Generic Issue 94, 'Additional Low-Temperature Overpressure for Light-Water Reactors,' Pursuant to 10 CFR 50.54(f)," June 25, 1990.]

B 3.4 REACTOR COOLANT SYSTEM (RCS)

B 3.4.12 Low Temperature Overpressure Protection (LTOP) System

BASES

BACKGROUND

The LTOP System controls RCS pressure at low temperatures so the integrity of the reactor coolant pressure boundary (RCPB) is not compromised by violating the pressure and temperature (P/T) limits of 10 CFR 50, Appendix G (Ref. 1). The reactor vessel is the limiting RCPB component for demonstrating such protection. LCO 3.4.3, "RCS Pressure and Temperature (P/T) Limits," provides the allowable combinations for operational pressure and temperature during cooldown, shutdown, and heatup to keep from violating the Reference 1 requirements during the LTOP MODES.

The reactor vessel material is less tough at low temperatures than at normal operating temperatures. As the vessel neutron exposure accumulates, the material toughness decreases and becomes less resistant to pressure stress at low temperatures (Ref. 2). RCS pressure, therefore, is maintained low at low temperatures and is increased only as temperature is increased.

The potential for vessel overpressurization is most acute when the RCS is water solid, occurring only while shutdown; a pressure fluctuation can occur more quickly than an operator can react to relieve the condition. Exceeding the RCS P/T limits by a significant amount could cause brittle cracking of the reactor vessel. LCO 3.4.3 requires administrative control of RCS pressure and temperature during heatup and cooldown to prevent exceeding the P/T limits.

This LCO provides RCS overpressure protection by having a minimum coolant input capability and having adequate pressure relief capacity. Limiting coolant input capability requires all but one high pressure safety injection (HPSI) pump and one charging pump incapable of injection into the RCS and isolating the safety injection tanks (SITs). The pressure relief capacity requires either two OPERABLE redundant power operated relief valves (PORVs) or the RCS depressurized and an RCS vent of sufficient size. One PORV or the RCS vent is the overpressure protection device that acts to terminate an increasing pressure event.

BASES

BACKGROUND (continued)

With minimum coolant input capability, the ability to provide core coolant addition is restricted. The LCO does not require the makeup control system deactivated or the safety injection (SI) actuation circuits blocked. Due to the lower pressures in the LTOP MODES and the expected core decay heat levels, the makeup system can provide adequate flow via the makeup control valve. If conditions require the use of more than one [HPI or] charging pump for makeup in the event of loss of inventory, then pumps can be made available through manual actions.

The LTOP System for pressure relief consists of two PORVs with reduced lift settings or an RCS vent of sufficient size. Two relief valves are required for redundancy. One PORV has adequate relieving capability to prevent overpressurization for the required coolant input capability.

PORV Requirements

As designed for the LTOP System, each PORV is signaled to open if the RCS pressure approaches a limit determined by the LTOP actuation logic. The actuation logic monitors RCS pressure and determines when the LTOP overpressure setting is approached. If the indicated pressure meets or exceeds the calculated value, a PORV is signaled to open.

The LCO presents the PORV setpoints for LTOP. The setpoints are normally staggered so only one valve opens during a low temperature overpressure transient. Having the setpoints of both valves within the limits of the LCO ensures the P/T limits will not be exceeded in any analyzed event.

When a PORV is opened in an increasing pressure transient, the release of coolant causes the pressure increase to slow and reverse. As the PORV releases coolant, the system pressure decreases until a reset pressure is reached and the valve is signaled to close. The pressure continues to decrease below the reset pressure as the valve closes.

RCS Vent Requirements

Once the RCS is depressurized, a vent exposed to the containment atmosphere will maintain the RCS at containment ambient pressure in an RCS overpressure transient, if the relieving requirements of the transient do not exceed the capabilities of the vent. Thus, the vent path must be capable of relieving the flow resulting from the limiting LTOP mass or heat input transient and maintaining pressure below the P/T limits. The required vent capacity may be provided by one or more vent paths.

BASES

BACKGROUND (continued)

For an RCS vent to meet the specified flow capacity, it requires removing a pressurizer safety valve, removing a PORV's internals, and disabling its block valve in the open position, or similarly establishing a vent by opening an RCS vent valve. The vent path(s) must be above the level of reactor coolant, so as not to drain the RCS when open.

APPLICABLE SAFETY ANALYSES

Safety analyses (Ref. 3) demonstrate that the reactor vessel is adequately protected against exceeding the Reference 1 P/T limits during shutdown. In MODES 1, 2, and 3, and in MODE 4 with any RCS cold leg temperature greater than the LTOP enable temperature specified in the PTLR, the pressurizer safety valves prevent RCS pressure from exceeding the Reference 1 limits. At the LTOP enable temperature specified in the PTLR and below, overpressure prevention falls to the OPERABLE PORVs [or to a depressurized RCS and a sufficient sized RCS vent]. Each of these means has a limited overpressure relief capability.

The actual temperature at which the pressure in the P/T limit curve falls below the pressurizer safety valve setpoint increases as the reactor vessel material toughness decreases due to neutron embrittlement. Each time the P/T limit curves are revised, the LTOP System will be re-evaluated to ensure its functional requirements can still be satisfied using the PORV method or the depressurized and vented RCS condition.

Reference 3 contains the acceptance limits that satisfy the LTOP requirements. Any change to the RCS must be evaluated against these analyses to determine the impact of the change on the LTOP acceptance limits.

Transients that are capable of overpressurizing the RCS are categorized as either mass or heat input transients, examples of which follow:

<u>Mass Input Type Transients</u>

a. Inadvertent safety injection or

b. Charging/letdown flow mismatch.

<u>Heat Input Type Transients</u>

a. Inadvertent actuation of pressurizer heaters,

b. Loss of shutdown cooling (SDC), or

BASES

APPLICABLE SAFETY ANALYSES (continued)

c. Reactor coolant pump (RCP) startup with temperature asymmetry within the RCS or between the RCS and steam generators.

The following are required during the LTOP MODES to ensure that mass and heat input transients do not occur, which either of the LTOP overpressure protection means cannot handle:

a. Rendering all but one HPSI pump, and all but one charging pump incapable of injection and

b. Deactivating the SIT discharge isolation valves in their closed positions.

The Reference 3 analyses demonstrate that either one PORV or the RCS vent can maintain RCS pressure below limits when only one HPSI pump and one charging pump are actuated. Thus, the LCO allows only one HPSI pump and one charging pump OPERABLE during the LTOP MODES. Since neither the PORV nor the RCS vent can handle the pressure transient produced from accumulator injection, when RCS temperature is low, the LCO also requires the SITs isolation when accumulator pressure is greater than or equal to the maximum RCS pressure for the existing RCS cold leg temperature allowed in the PTLR.

The isolated SITs must have their discharge valves closed and the valve power supply breakers fixed in their open positions. The analyses show the effect of SIT discharge is over a narrower RCS temperature range ([175]°F and below) than that of the LCO (less than or equal to the LTOP enable temperature specified in the PTLR and below).

Fracture mechanics analyses established the temperature of LTOP Applicability at less than or equal to the LTOP enable temperature specified in the PTLR. Above this temperature, the pressurizer safety valves provide the reactor vessel pressure protection. The vessel materials were assumed to have a neutron irradiation accumulation equal to 21 effective full power years of operation.

The consequences of a small break loss of coolant accident (LOCA) in LTOP MODE 4 conform to 10 CFR 50.46 and 10 CFR 50, Appendix K (Refs. 4 and 5), requirements by having a maximum of one HPSI pump and one charging pump OPERABLE and SI actuation enabled for these pumps.

BASES

APPLICABLE SAFETY ANALYSES (continued)

PORV Performance

The fracture mechanics analyses show that the vessel is protected when the PORVs are set to open at or below the limits specified in the PTLR. The setpoint is derived by modeling the performance of the LTOP System, assuming the limiting allowed LTOP transient of one HPSI pump and one charging pump injecting into the RCS. These analyses consider pressure overshoot and undershoot beyond the PORV opening and closing setpoints, resulting from signal processing and valve stroke times. The PORV setpoints at or below the derived limit ensure the Reference 1 limits will be met.

The PORV setpoints will be re-evaluated for compliance when the revised P/T limits conflict with the LTOP analysis limits. The P/T limits are periodically modified as the reactor vessel material toughness decreases due to embrittlement caused by neutron irradiation. Revised P/T limits are determined using neutron fluence projections and the results of examinations of the reactor vessel material irradiation surveillance specimens. The Bases for LCO 3.4.3, "RCS Pressure and Temperature (P/T) Limits," discuss these examinations.

The PORVs are considered active components. Thus, the failure of one PORV represents the worst case, single active failure.

RCS Vent Performance

With the RCS depressurized, analyses show a vent size of [1.3] square inches is capable of mitigating the limiting allowed LTOP overpressure transient. In that event, this size vent maintains RCS pressure less than the maximum RCS pressure on the P/T limit curve.

The RCS vent size will also be re-evaluated for compliance each time the P/T limit curves are revised based on the results of the vessel material surveillance.

The RCS vent is passive and is not subject to active failure.

LTOP System satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO

This LCO is required to ensure that the LTOP System is OPERABLE. The LTOP System is OPERABLE when the minimum coolant input and pressure relief capabilities are OPERABLE. Violation of this LCO could lead to the loss of low temperature overpressure mitigation and violation of the Reference 1 limits as a result of an operational transient.

To limit the coolant input capability, the LCO requires that a maximum of one HPSI pump and one charging pump be capable of injecting into the RCS, and the SITs isolated (when accumulator pressure is greater than or equal to the maximum RCS pressure for the existing RCS cold leg temperature allowed in the PTLR).

The LCO is modified by two Notes. Note 1 allows [two charging pumps] to be made capable of injecting for ≤ 1 hour during pump swap operations. One hour provides sufficient time to safely complete the actual transfer and to complete the administrative controls and Surveillance Requirements associated with the swap. The intent is to minimize the actual time that more than [one] charging pump is physically capable of injection. Note 2 states that SIT isolation is only required when the SIT pressure is greater than or equal to the RCS pressure for the existing temperature, as allowed by the P/T limit curves provided in the PTLR. This Note permits the SIT discharge valve surveillance performed only under these pressure and temperature conditions.

The elements of the LCO that provide overpressure mitigation through pressure relief are:

a. Two OPERABLE PORVs or

b. The depressurized RCS and an RCS vent.

A PORV is OPERABLE for LTOP when its block valve is open, its lift setpoint is set within the limits specified in the PTLR and testing has proven its ability to open at that setpoint, and motive power is available to the two valves and their control circuits.

An RCS vent is OPERABLE when open with an area ≥ [1.3] square inches.

Each of these methods of overpressure prevention is capable of mitigating the limiting LTOP transient.

BASES

APPLICABILITY

This LCO is applicable in MODE 4 when the temperature of any RCS cold leg is less than or equal to the LTOP enable temperature specified in the PTLR, in MODE 5, and in MODE 6 when the reactor vessel head is on. The pressurizer safety valves provide overpressure protection that meets the Reference 1 P/T limits above the LTOP enable temperature and below. When the reactor vessel head is off, overpressurization cannot occur.

LCO 3.4.3 provides the operational P/T limits for all MODES.
LCO 3.4.10, "Pressurizer Safety Valves," requires the OPERABILITY of the pressurizer safety valves that provide overpressure protection during MODES 1, 2, and 3, and MODE 4 above the LTOP enable temperature specified in the PTLR.

Low temperature overpressure prevention is most critical during shutdown when the RCS is water solid, and a mass or heat input transient can cause a very rapid increase in RCS pressure when little or no time allows operator action to mitigate the event.

ACTIONS

A Note prohibits the application of LCO 3.0.4.b to inoperable PORVs used for LTOP. There is an increased risk associated with entering MODE 4 from MODE 5 with PORVs used for LTOP inoperable and the provisions of LCO 3.0.4.b, which allow entry into a MODE or other specified condition in the Applicability with the LCO not met after performance of a risk assessment addressing inoperable systems and components, should not be applied in this circumstance.

A.1 and B.1

With two or more HPSI pumps capable of injecting into the RCS, overpressurization is possible.

The immediate Completion Time to initiate actions to restore restricted coolant input capability to the RCS reflects the importance of maintaining overpressure protection of the RCS.

C.1, D.1, and D.2

An unisolated SIT requires isolation within 1 hour. This is only required when the SIT pressure is greater than or equal to the maximum RCS pressure for the existing cold leg temperature allowed in the PTLR.

BASES

ACTIONS (continued)

If isolation is needed and cannot be accomplished within 1 hour, Required Action D.1 and Required Action D.2 provide two options, either of which must be performed within 12 hours. By increasing the RCS temperature to > [175]°F, a SIT pressure of [600] psig cannot exceed the LTOP limits if the tanks are fully injected. Depressurizing the SIT below the LTOP limit stated in the PTLR also protects against such an event.

The Completion Times are based on operating experience that these activities can be accomplished in these time periods and on engineering evaluations indicating that an event requiring LTOP is not likely in the allowed times.

E.1

In MODE 4 when any RCS cold leg temperature is ≤ [285]°F, with one PORV inoperable, two PORVs must be restored to OPERABLE status within a Completion Time of 7 days. Two valves are required to meet the LCO requirement and to provide low temperature overpressure mitigation while withstanding a single failure of an active component.

The Completion Time is based on the facts that only one PORV is required to mitigate an overpressure transient and that the likelihood of an active failure of the remaining valve path during this time period is very low.

F.1

The consequences of operational events that will overpressure the RCS are more severe at lower temperature (Ref. 6). Thus, one required PORV inoperable in MODE 5 or in MODE 6 with the head on, the Completion Time to restore two valves to OPERABLE status is 24 hours.

The 24 hour Completion Time to restore two PORVs OPERABLE in MODE 5 or in MODE 6 when the vessel head is on is a reasonable amount of time to investigate and repair several types of PORV failures without exposure to a lengthy period with only one PORV OPERABLE to protect against overpressure events.

BASES

ACTIONS (continued)

G.1

If two required PORVs are inoperable, or if a Required Action and the associated Completion Time of Condition A, B, D, E, or F are not met, or if the LTOP System is inoperable for any reason other than Condition A through Condition F, the RCS must be depressurized and a vent established within 12 hours. The vent must be sized at least [1.3] square inches to ensure the flow capacity is greater than that required for the worst case mass input transient reasonable during the applicable MODES. This action protects the RCPB from a low temperature overpressure event and a possible brittle failure of the reactor vessel.

The Completion Time of 12 hours to depressurize and vent the RCS is based on the time required to place the plant in this condition and the relatively low probability of an overpressure event during this time period due to increased operator awareness of administrative control requirements.

SURVEILLANCE REQUIREMENTS

SR 3.4.12.1, SR 3.4.12.2, and SR 3.4.12.3

To minimize the potential for a low temperature overpressure event by limiting the mass input capability, only one HPSI pump and all but [one] charging pump are verified OPERABLE with the other pumps locked out with power removed and the SIT discharge incapable of injecting into the RCS. The [HPI] pump[s] and charging pump[s] are rendered incapable of injecting into the RCS through removing the power from the pumps by racking the breakers out under administrative control. An alternate method of LTOP control may be employed using at least two independent means to prevent a pump start such that a single failure or single action will not result in an injection into the RCS. This may be accomplished through the pump control switch being placed in [pull to lock] and at least one valve in the discharge flow path being closed.

The 12 hour interval considers operating practice to regularly assess potential degradation and to verify operation within the safety analysis.

SR 3.4.12.4

SR 3.4.12.4 requires verifying that the required RCS vent is open ≥ [1.3] square inches is proven OPERABLE by verifying its open condition either:

BASES

SURVEILLANCE REQUIREMENTS (continued)

a. Once every 12 hours for a valve that is unlocked open (valves that are sealed or secured in the open position are considered "locked" in this context) or

b. Once every 31 days for other vent path(s) (e.g., a vent valve that is locked, sealed, or secured in position, a removed pressurizer safety valve, or open manway).

The passive vent path arrangement must only be open to be OPERABLE. This Surveillance need only be performed if the vent is being used to satisfy the requirements of this LCO. The Frequencies consider operating experience with mispositioning of unlocked and locked vent valves, respectively.

SR 3.4.12.5

The PORV block valve must be verified open every 72 hours to provide the flow path for each required PORV to perform its function when actuated. The valve can be remotely verified open in the main control room.

The block valve is a remotely controlled, motor operated valve. The power to the valve motor operator is not required to be removed, and the manual actuator is not required locked in the inactive position. Thus, the block valve can be closed in the event the PORV develops excessive leakage or does not close (sticks open) after relieving an overpressure event.

The 72 hour Frequency considers operating experience with accidental movement of valves having remote control and position indication capabilities available where easily monitored. These considerations include the administrative controls over main control room access and equipment control.

SR 3.4.12.6

Performance of a CHANNEL FUNCTIONAL TEST is required every 31 days to verify and, as necessary, adjust the PORV open setpoints. The CHANNEL FUNCTIONAL TEST will verify on a monthly basis that the PORV lift setpoints are within the LCO limit. A successful test of the required contact(s) of a channel relay may be performed by the

BASES

SURVEILLANCE REQUIREMENTS (continued)

verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions. PORV actuation could depressurize the RCS and is not required. The 31 day Frequency considers experience with equipment reliability.

A Note has been added indicating this SR is required to be performed [12] hours after decreasing RCS cold leg temperature to less than or equal to the LTOP enable temperature specified in the PTLR. The test cannot be performed until the RCS is in the LTOP MODES when the PORV lift setpoint can be reduced to the LTOP setting. The test must be performed within 12 hours after entering the LTOP MODES.

SR 3.4.12.7

Performance of a CHANNEL CALIBRATION on each required PORV actuation channel is required every [18] months to adjust the whole channel so that it responds and the valve opens within the required LTOP range and with accuracy to known input.

The [18] month Frequency considers operating experience with equipment reliability and matches the typical refueling outage schedule.

REFERENCES

1. 10 CFR 50, Appendix G.
2. Generic Letter 88-11.
3. FSAR, Section [15].
4. 10 CFR 50.46.
5. 10 CFR 50, Appendix K.
6. Generic Letter 90-06.

B 3.4 REACTOR COOLANT SYSTEM (RCS)

B 3.4.13 RCS Operational LEAKAGE

BASES

BACKGROUND

Components that contain or transport the coolant to or from the reactor core make up the RCS. Component joints are made by welding, bolting, rolling, or pressure loading, and valves isolate connecting systems from the RCS.

During plant life, the joint and valve interfaces can produce varying amounts of reactor coolant LEAKAGE, through either normal operational wear or mechanical deterioration. The purpose of the RCS Operational LEAKAGE LCO is to limit system operation in the presence of LEAKAGE from these sources to amounts that do not compromise safety. This LCO specifies the types and amounts of LEAKAGE.

10 CFR 50, Appendix A, GDC 30 (Ref. 1), requires means for detecting and, to the extent practical, identifying the source of reactor coolant LEAKAGE. Regulatory Guide 1.45 (Ref. 2) describes acceptable methods for selecting leakage detection systems.

The safety significance of RCS LEAKAGE varies widely depending on its source, rate, and duration. Therefore, detecting and monitoring reactor coolant LEAKAGE into the containment area is necessary. Quickly separating the identified LEAKAGE from the unidentified LEAKAGE is necessary to provide quantitative information to the operators, allowing them to take corrective action should a leak occur detrimental to the safety of the facility and the public.

A limited amount of leakage inside containment is expected from auxiliary systems that cannot be made 100% leaktight. Leakage from these systems should be detected, located, and isolated from the containment atmosphere, if possible, to not interfere with RCS LEAKAGE detection.

This LCO deals with protection of the reactor coolant pressure boundary (RCPB) from degradation and the core from inadequate cooling, in addition to preventing the accident analysis radiation release assumptions from being exceeded. The consequences of violating this LCO include the possibility of a loss of coolant accident (LOCA).

BASES

APPLICABLE SAFETY ANALYSES

Except for primary to secondary LEAKAGE, the safety analyses do not address operational LEAKAGE. However, other operational LEAKAGE is related to the safety analyses for LOCA; the amount of leakage can affect the probability of such an event. The safety analysis for an event resulting in steam discharge to the atmosphere assumes that primary to secondary LEAKAGE from all steam generators (SGs) is [1 gallon per minute] or increases to [1 gallon per minute] as a result of accident induced conditions. The LCO requirement to limit primary to secondary LEAKAGE through any one SG to less than or equal to 150 gallons per day is significantly less than the conditions assumed in the safety analysis.

Primary to secondary LEAKAGE is a factor in the dose releases outside containment resulting from a steam line break (SLB) accident. To a lesser extent, other accidents or transients involve secondary steam release to the atmosphere, such as a steam generator tube rupture (SGTR). The leakage contaminates the secondary fluid.

The FSAR (Ref. 3) analysis for SGTR assumes the contaminated secondary fluid is only briefly released via safety valves and the majority is steamed to the condenser. The [1 gpm] primary to secondary LEAKAGE safety analysis assumption is relatively inconsequential.

The SLB is more limiting for site radiation releases. The safety analysis for the SLB accident assumes the entire [1 gpm] primary to secondary LEAKAGE is through the affected generator as an initial condition. The dose consequences resulting from the SLB accident are well within the limits defined in 10 CFR 50 or the staff approved licensing basis (i.e., a small fraction of these limits).

RCS operational LEAKAGE satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

RCS operational LEAKAGE shall be limited to:

a. Pressure Boundary LEAKAGE

No pressure boundary LEAKAGE is allowed, being indicative of material deterioration. LEAKAGE of this type is unacceptable as the leak itself could cause further deterioration, resulting in higher LEAKAGE. Violation of this LCO could result in continued degradation of the RCPB. LEAKAGE past seals and gaskets is not pressure boundary LEAKAGE.

BASES

LCO (continued)

b. Unidentified LEAKAGE

One gallon per minute (gpm) of unidentified LEAKAGE is allowed as a reasonable minimum detectable amount that the containment air monitoring and containment sump level monitoring equipment can detect within a reasonable time period. Violation of this LCO could result in continued degradation of the RCPB, if the LEAKAGE is from the pressure boundary.

c. Identified LEAKAGE

Up to 10 gpm of identified LEAKAGE is considered allowable because LEAKAGE is from known sources that do not interfere with detection of unidentified LEAKAGE and is well within the capability of the RCS makeup system. Identified LEAKAGE includes LEAKAGE to the containment from specifically known and located sources, but does not include pressure boundary LEAKAGE or controlled reactor coolant pump (RCP) seal leakoff (a normal function not considered LEAKAGE). Violation of this LCO could result in continued degradation of a component or system.

LCO 3.4.14, "RCS Pressure Isolation Valve (PIV) Leakage," measures leakage through each individual PIV and can impact this LCO. Of the two PIVs in series in each isolated line, leakage measured through one PIV does not result in RCS LEAKAGE when the other is leaktight. If both valves leak and result in a loss of mass from the RCS, the loss must be included in the allowable identified LEAKAGE.

d. Primary to Secondary LEAKAGE Through Any One SG

The limit of 150 gallons per day per SG is based on the operational LEAKAGE performance criterion in NEI 97-06, Steam Generator Program Guidelines (Ref. 4). The Steam Generator Program operational LEAKAGE performance criterion in NEI 97-06 states, "The RCS operational primary to secondary leakage through any one SG shall be limited to 150 gallons per day." The limit is based on operating experience with SG tube degradation mechanisms that result in tube leakage. The operational leakage rate criterion in conjunction with the implementation of the Steam Generator Program is an effective measure for minimizing the frequency of steam generator tube ruptures.

BASES

APPLICABILITY

In MODES 1, 2, 3, and 4, the potential for RCPB LEAKAGE is greatest when the RCS is pressurized.

In MODES 5 and 6, LEAKAGE limits are not required because the reactor coolant pressure is far lower, resulting in lower stresses and reduced potentials for LEAKAGE.

ACTIONS

A.1

Unidentified LEAKAGE or identified LEAKAGE in excess of the LCO limits must be reduced to within limits within 4 hours. This Completion Time allows time to verify leakage rates and either identify unidentified LEAKAGE or reduce LEAKAGE to within limits before the reactor must be shut down. This action is necessary to prevent further deterioration of the RCPB.

B.1 and B.2

If any pressure boundary LEAKAGE exists or primary to secondary LEAKAGE is not within limit, or if unidentified or identified LEAKAGE cannot be reduced to within limits within 4 hours, the reactor must be brought to lower pressure conditions to reduce the severity of the LEAKAGE and its potential consequences. The reactor must be brought to MODE 3 within 6 hours and to MODE 5 within 36 hours. This action reduces the LEAKAGE and also reduces the factors that tend to degrade the pressure boundary.

The allowed Completion Times are reasonable, based on operating experience, to reach the required conditions from full power conditions in an orderly manner and without challenging plant systems. In MODE 5, the pressure stresses acting on the RCPB are much lower, and further deterioration is much less likely.

SURVEILLANCE REQUIREMENTS

SR 3.4.13.1

Verifying RCS LEAKAGE to be within the LCO limits ensures the integrity of the RCPB is maintained. Pressure boundary LEAKAGE would at first appear as unidentified LEAKAGE and can only be positively identified by inspection. Unidentified LEAKAGE and identified LEAKAGE are determined by performance of an RCS water inventory balance.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The RCS water inventory balance must be performed with the reactor at steady state operating conditions (stable temperature, power level, pressurizer and makeup tank levels, makeup and letdown, [and RCP seal injection and return flows]). The Surveillance is modified by two Notes. Note 1 states that this SR is not required to be performed until 12 hours after establishing steady state operation. The 12 hour allowance provides sufficient time to collect and process all necessary data after stable plant conditions are established.

Steady state operation is required to perform a proper water inventory balance since calculations during maneuvering are not useful. For RCS operational LEAKAGE determination by water inventory balance, steady state is defined as stable RCS pressure, temperature, power level, pressurizer and makeup tank levels, makeup and letdown, and RCP seal injection and return flows.

An early warning of pressure boundary LEAKAGE or unidentified LEAKAGE is provided by the automatic systems that monitor the containment atmosphere radioactivity and the containment sump level. These leakage detection systems are specified in LCO 3.4.15, "RCS Leakage Detection Instrumentation."

Note 2 states that this SR is not applicable to primary to secondary LEAKAGE because LEAKAGE of 150 gallons per day cannot be measured accurately by an RCS water inventory balance.

The 72 hour Frequency is a reasonable interval to trend LEAKAGE and recognizes the importance of early leakage detection in the prevention of accidents.

SR 3.4.13.2

This SR verifies that primary to secondary LEAKAGE is less or equal to 150 gallons per day through any one SG. Satisfying the primary to secondary LEAKAGE limit ensures that the operational LEAKAGE performance criterion in the Steam Generator Program is met. If this SR is not met, compliance with LCO 3.4.18, "Steam Generator Tube Integrity," should be evaluated. The 150 gallons per day limit is measured at room temperature as described in Reference 5. The operational LEAKAGE rate limit applies to LEAKAGE through any one SG. If it is not practical to assign the LEAKAGE to an individual SG, all the primary to secondary LEAKAGE should be conservatively assumed to be from one SG.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The Surveillance is modified by a Note which states that the Surveillance is not required to be performed until 12 hours after establishment of steady state operation. For RCS primary to secondary LEAKAGE determination, steady state is defined as stable RCS pressure, temperature, power level, pressurizer and makeup tank levels, makeup and letdown, and RCP seal injection and return flows.

The Surveillance Frequency of 72 hours is a reasonable interval to trend primary to secondary LEAKAGE and recognizes the importance of early leakage detection in the prevention of accidents. The primary to secondary LEAKAGE is determined using continuous process radiation monitors or radiochemical grab sampling in accordance with the EPRI guidelines (Ref. 5).

REFERENCES

1. 10 CFR 50, Appendix A, GDC 30.
2. Regulatory Guide 1.45, May 1973.
3. FSAR, Section [15].
4. NEI 97-06, "Steam Generator Program Guidelines."
5. EPRI, "Pressurized Water Reactor Primary-to-Secondary Leak Guidelines."

B 3.4 REACTOR COOLANT SYSTEM (RCS)

B 3.4.14 RCS Pressure Isolation Valve (PIV) Leakage

BASES

BACKGROUND

10 CFR 50.2, 10 CFR 50.55a(c), and GDC 55 of 10 CFR 50, Appendix A (Refs. 1, 2, and 3), define RCS PIVs as any two normally closed valves in series within the RCS pressure boundary that separate the high pressure RCS from an attached low pressure system. During their lives, these valves can produce varying amounts of reactor coolant leakage through either normal operational wear or mechanical deterioration. The RCS PIV LCO allows RCS high pressure operation when leakage through these valves exists in amounts that do not compromise safety.

The PIV leakage limit applies to each individual valve. Leakage through both PIVs in series in a line must be included as part of the identified LEAKAGE, governed by LCO 3.4.13, "RCS Operational LEAKAGE." This is true during operation only when the loss of RCS mass through two valves in series is determined by a water inventory balance (SR 3.4.13.1). A known component of the identified LEAKAGE before operation begins is the least of the two individual leakage rates determined for leaking series PIVs during the required surveillance testing; leakage measured through one PIV in a line is not RCS operational LEAKAGE if the other is leaktight.

Although this specification provides a limit on allowable PIV leakage rate, its main purpose is to prevent overpressure failure of the low pressure portions of connecting systems. The leakage limit is an indication that the PIVs between the RCS and the connecting systems are degraded or degrading. PIV leakage could lead to overpressure of the low pressure piping or components. Failure consequences could be a loss of coolant accident (LOCA) outside of containment, an unanalyzed condition that could degrade the ability for low pressure injection.

The basis for this LCO is the 1975 NRC "Reactor Safety Study" (Ref. 4) that identified potential intersystem LOCAs as a significant contributor to the risk of core melt. A subsequent study (Ref. 5) evaluated various PIV configurations to determine the probability of intersystem LOCAs.

PIVs are provided to isolate the RCS from the following typically connected systems:

BASES

BACKGROUND (continued)

a. Shutdown Cooling (SDC) System,

b. Safety Injection System, and

c. Chemical and Volume Control System.

The PIVs are listed in FSAR section (Ref. 6).

Violation of this LCO could result in continued degradation of a PIV, which could lead to overpressurization of a low pressure system and the loss of the integrity of a fission product barrier.

APPLICABLE SAFETY ANALYSES

Reference 4 identified potential intersystem LOCAs as a significant contributor to the risk of core melt. The dominant accident sequence in the intersystem LOCA category is the failure of the low pressure portion of the SDC System outside of containment. The accident is the result of a postulated failure of the PIVs, which are part of the reactor coolant pressure boundary (RCPB), and the subsequent pressurization of the SDC System downstream of the PIVs from the RCS. Because the low pressure portion of the SDC System is typically designed for [600] psig, overpressurization failure of the SDC low pressure line would result in a LOCA outside containment and subsequent risk of core melt.

Reference 5 evaluated various PIV configurations, leakage testing of the valves, and operational changes to determine the effect on the probability of intersystem LOCAs. This study concluded that periodic leakage testing of the PIVs can substantially reduce the probability of an intersystem LOCA.

RCS PIV leakage satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

RCS PIV leakage is identified LEAKAGE into closed systems connected to the RCS. Isolation valve leakage is usually on the order of drops per minute. Leakage that increases significantly suggests that something is operationally wrong and corrective action must be taken.

The LCO PIV leakage limit is 0.5 gpm per nominal inch of valve size, with a maximum limit of 5 gpm. The previous criterion of 1 gpm for all valve sizes imposed an unjustified penalty on the larger valves without providing information on potential valve degradation and resulted in higher personnel radiation exposures. A study concluded a leakage rate limit based on valve size was superior to a single allowable value.

BASES

LCO (continued)

Reference 7 permits leakage testing at a lower pressure differential than between the specified maximum RCS pressure and the normal pressure of the connected system during RCS operation (the maximum pressure differential) in those types of valves in which the higher service pressure will tend to diminish the overall leakage channel opening. In such cases, the observed rate may be adjusted to the maximum pressure differential by assuming leakage is directly proportional to the pressure differential to the one half power.

APPLICABILITY

In MODES 1, 2, 3, and 4, this LCO applies because the PIV leakage potential is greatest when the RCS is pressurized. In MODE 4, valves in the SDC flow path are not required to meet the requirements of this LCO when in, or during the transition to or from, the SDC mode of operation.

In MODES 5 and 6, leakage limits are not provided because the lower reactor coolant pressure results in a reduced potential for leakage and for a LOCA outside the containment.

ACTIONS

The Actions are modified by two Notes. Note 1 is added to provide clarification that each flow path allows separate entry into a Condition. This is allowed based on the functional independence of the flow path. Note 2 requires an evaluation of affected systems if a PIV is inoperable. The leakage may have affected system operability or isolation of a leaking flow path with an alternate valve may have degraded the ability of the interconnected system to perform its safety function.

<u>A.1 and A.2</u>

The flow path must be isolated by two valves. Required Actions A.1 and A.2 are modified by a Note stating that the valves used for isolation must meet the same leakage requirements as the PIVs and must be in the RCPB [or the high pressure portion of the system].

Required Action A.1 requires that the isolation with one valve must be performed within 4 hours. Four hours provides time to reduce leakage in excess of the allowable limit and to isolate if leakage cannot be reduced. The 4 hours allows the actions and restricts the operation with leaking isolation valves.

BASES

ACTIONS (continued)

[Required Action A.2 specifies that the double isolation barrier of two valves be restored by closing some other valve qualified for isolation or restoring one leaking PIV. The 72 hour Completion Time after exceeding the limit considers the time required to complete the action and the low probability of a second valve failing during this time period.

or

The 72 hour Completion Time after exceeding the limit allows for the restoration of the leaking PIV to OPERABLE status. This timeframe considers the time required to complete this Action and the low probability of a second valve failing during this period.]

-----------------------------------REVIEWER'S NOTE-----------------------------------
Two options are provided for Required Action A.2. The second option (72 hour restoration) is appropriate if isolation of a second valve would place the unit in an unanalyzed condition.

B.1 and B.2

If leakage cannot be reduced [the system isolated] or other Required Actions accomplished, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to MODE 3 within 6 hours and to MODE 5 within 36 hours. This Action reduces the leakage and also reduces the potential for a LOCA outside the containment. The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

C.1

The inoperability of the SDC autoclosure interlock renders the SDC suction isolation valves incapable of: isolating in response to a high pressure condition and preventing inadvertent opening of the valves at RCS pressures in excess of the SDC systems design pressure. If the SDC autoclosure interlock is inoperable, operation may continue as long as the affected SDC suction penetration is closed by at least one closed manual or deactivated automatic valve within 4 hours. This Action accomplishes the purpose of the autoclosure function.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.4.14.1

Performance of leakage testing on each RCS PIV or isolation valve used to satisfy Required Action A.1 or A.2 is required to verify that leakage is below the specified limit and to identify each leaking valve. The leakage limit of 0.5 gpm per inch of nominal valve diameter up to 5 gpm maximum applies to each valve. Leakage testing requires a stable pressure condition.

For the two PIVs in series, the leakage requirement applies to each valve individually and not to the combined leakage across both valves. If the PIVs are not individually leakage tested, one valve may have failed completely and not be detected if the other valve in series meets the leakage requirement. In this situation, the protection provided by redundant valves would be lost.

Testing is to be performed every 9 months, but may be extended up to a maximum of [18] months, a typical refueling cycle, if the plant does not go into MODE 5 for at least 7 days. The [18] month Frequency is consistent with 10 CFR 50.55a(g) (Ref. 8), as contained in the Inservice Testing Program, is within frequency allowed by the American Society of Mechanical Engineers (ASME) Code (Ref. 7), and is based on the need to perform the Surveillance under conditions that apply during a plant outage and the potential for an unplanned transient if the Surveillance were performed with the reactor at power.

In addition, testing must be performed once after the valve has been opened by flow or exercised to ensure tight reseating. PIVs disturbed in the performance of this Surveillance should also be tested unless documentation shows that an infinite testing loop cannot practically be avoided. Testing must be performed within 24 hours after the valve has been reseated. Within 24 hours is a reasonable and practical time limit for performing this test after opening or reseating a valve.

The leakage limit is to be met at the RCS pressure associated with MODES 1 and 2. This permits leakage testing at high differential pressures with stable conditions not possible in the MODES with lower pressures.

Entry into MODES 3 and 4 is allowed to establish the necessary differential pressures and stable conditions to allow for performance of this Surveillance. The Note that allows this provision is complimentary to the Frequency of prior to entry into MODE 2 whenever the unit has been in MODE 5 for 7 days or more, if leakage testing has not been performed

BASES

SURVEILLANCE REQUIREMENTS (continued)

in the previous 9 months. In addition, this Surveillance is not required to be performed on the SDC System when the SDC System is aligned to the RCS in the shutdown cooling mode of operation. PIVs contained in the SDC shutdown cooling flow path must be leakage rate tested after SDC is secured and stable unit conditions and the necessary differential pressures are established.

SR 3.4.14.2 and SR 3.4.14.3

Verifying that the SDC autoclosure interlocks are OPERABLE ensures that RCS pressure will not pressurize the SDC system beyond 125% of its design pressure of [600] psig. The interlock setpoint that prevents the valves from being opened is set so the actual RCS pressure must be < [425] psig to open the valves. This setpoint ensures the SDC design pressure will not be exceeded and the SDC relief valves will not lift. The 18 month Frequency is based on the need to perform these Surveillances under conditions that apply during a plant outage. The 18 month Frequency is also acceptable based on consideration of the design reliability (and confirming operating experience) of the equipment.

The SRs are modified by Notes allowing the SDC autoclosure function to be disabled when using the SDC System suction relief valves for cold overpressure protection in accordance with SR 3.4.12.7.

REFERENCES

1. 10 CFR 50.2.
2. 10 CFR 50.55a(c).
3. 10 CFR 50, Appendix A, Section V, GDC 55.
4. WASH-1400 (NUREG-75/014), Appendix V, October 1975.
5. NUREG-0677, May 1980.
6. [Document containing list of PIVs.]
7. ASME Code for Operation and Maintenance of Nuclear Power Plants.
8. 10 CFR 50.55a(g).

B 3.4 REACTOR COOLANT SYSTEM (RCS)

B 3.4.15 RCS Leakage Detection Instrumentation

BASES

BACKGROUND

GDC 30 of Appendix A to 10 CFR 50 (Ref. 1) requires means for detecting and, to the extent practical, identifying the location of the source of RCS LEAKAGE. Regulatory Guide 1.45 (Ref. 2) describes acceptable methods for selecting leakage detection systems.

Leakage detection systems must have the capability to detect significant reactor coolant pressure boundary (RCPB) degradation as soon after occurrence as practical to minimize the potential for propagation to a gross failure. Thus, an early indication or warning signal is necessary to permit proper evaluation of all unidentified LEAKAGE.

Industry practice has shown that water flow changes of 0.5 gpm to 1.0 gpm can readily be detected in contained volumes by monitoring changes in water level, in flow rate, or in the operating frequency of a pump. The containment sump used to collect unidentified LEAKAGE [is] and the containment air cooler condensate flow rate monitor [are] instrumented to alarm for increases of 0.5 gpm to 1.0 gpm in the normal flow rates. This sensitivity is acceptable for detecting increases in unidentified LEAKAGE.

The reactor coolant contains radioactivity that, when released to the containment, can be detected by radiation monitoring instrumentation. Reactor coolant radioactivity levels will be low during initial reactor startup and for a few weeks thereafter until activated corrosion products have been formed and fission products appear from fuel element cladding contamination or cladding defects. Instrument sensitivities of 10^{-9} μCi/cc radioactivity for particulate monitoring and of 10^{-6} μCi/cc radioactivity for gaseous monitoring are practical for these leakage detection systems. Radioactivity detection systems are included for monitoring both particulate and gaseous activities, because of their sensitivities and rapid responses to RCS LEAKAGE.

An increase in humidity of the containment atmosphere would indicate release of water vapor to the containment. Dew point temperature measurements can thus be used to monitor humidity levels of the containment atmosphere as an indicator of potential RCS LEAKAGE. A 1°F increase in dew point is well within the sensitivity range of available instruments.

BASES

BACKGROUND (continued)

Since the humidity level is influenced by several factors, a quantitative evaluation of an indicated leakage rate by this means may be questionable and should be compared to observed increases in liquid flow into or from the containment sump [and condensate flow from air coolers]. Humidity level monitoring is considered most useful as an indirect alarm or indication to alert the operator to a potential problem. Humidity monitors are not required by this LCO.

Air temperature and pressure monitoring methods may also be used to infer unidentified LEAKAGE to the containment. Containment temperature and pressure fluctuate slightly during plant operation, but a rise above the normally indicated range of values may indicate RCS LEAKAGE into the containment. The relevance of temperature and pressure measurements are affected by containment free volume and, for temperature, detector location. Alarm signals from these instruments can be valuable in recognizing rapid and sizable leakage to the containment. Temperature and pressure monitors are not required by this LCO.

APPLICABLE SAFETY ANALYSES

The need to evaluate the severity of an alarm or an indication is important to the operators, and the ability to compare and verify with indications from other systems is necessary. The system response times and sensitivities are described in the FSAR (Ref. 3). Multiple instrument locations are utilized, if needed, to ensure the transport delay time of the LEAKAGE from its source to an instrument location yields an acceptable overall response time.

The safety significance of RCS LEAKAGE varies widely depending on its source, rate, and duration. Therefore, detecting and monitoring RCS LEAKAGE into the containment area are necessary. Quickly separating the identified LEAKAGE from the unidentified LEAKAGE provides quantitative information to the operators, allowing them to take corrective action should leakage occur detrimental to the safety of the facility and the public.

RCS leakage detection instrumentation satisfies Criterion 1 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO

One method of protecting against large RCS LEAKAGE derives from the ability of instruments to rapidly detect extremely small leaks. This LCO requires instruments of diverse monitoring principles to be OPERABLE to provide a high degree of confidence that extremely small leaks are detected in time to allow actions to place the plant in a safe condition when RCS LEAKAGE indicates possible RCPB degradation.

The LCO is satisfied when monitors of diverse measurement means are available. Thus, the containment sump monitor, in combination with a particulate or gaseous radioactivity monitor [and a containment air cooler condensate flow rate monitor], provides an acceptable minimum.

APPLICABILITY

Because of elevated RCS temperature and pressure in MODES 1, 2, 3, and 4, RCS leakage detection instrumentation is required to be OPERABLE.

In MODE 5 or 6, the temperature is ≤ 200°F and pressure is maintained low or at atmospheric pressure. Since the temperatures and pressures are far lower than those for MODES 1, 2, 3, and 4, the likelihood of leakage and crack propagation is much smaller. Therefore, the requirements of this LCO are not applicable in MODES 5 and 6.

ACTIONS

A.1 and A.2

If the containment sump monitor is inoperable, no other form of sampling can provide the equivalent information.

However, the containment atmosphere radioactivity monitor will provide indications of changes in leakage. Together with the atmosphere monitor, the periodic surveillance for RCS water inventory balance, SR 3.4.13.1, must be performed at an increased frequency of 24 hours to provide information that is adequate to detect leakage. A Note is added allowing that SR 3.4.13.1 is not required to be performed until 12 hours after establishing steady state operation (stable temperature, power level, pressurizer and makeup tank levels, makeup and letdown, and [RCP seal injection and return flows]). The 12 hour allowance provides sufficient time to collect and process all necessary data after stable plant conditions are established.

Restoration of the sump monitor to OPERABLE status is required to regain the function in a Completion Time of 30 days after the monitor's failure. This time is acceptable considering the frequency and adequacy of the RCS water inventory balance required by Required Action A.1.

BASES

ACTIONS (continued)

B.1.1, B.1.2, B.2.1, and B.2.2

With both gaseous and particulate containment atmosphere radioactivity monitoring instrumentation channels inoperable, alternative action is required. Either grab samples of the containment atmosphere must be taken and analyzed, or water inventory balances, in accordance with SR 3.4.13.1, must be performed to provide alternate periodic information. With a sample obtained and analyzed or an inventory balance performed every 24 hours, the reactor may be operated for up to 30 days to allow restoration of at least one of the radioactivity monitors.

Alternatively, continued operation is allowed if the air cooler condensate flow rate monitoring system is OPERABLE, provided grab samples are taken or water inventory balance performed every 24 hours.

The 24 hour interval provides periodic information that is adequate to detect leakage. A Note is added allowing that SR 3.4.13.1 is not required to be performed until 12 hours after establishing steady state operation (stable temperature, power level, pressurizer and makeup tank levels, makeup and letdown, and [RCP seal injection and return flows]). The 12 hour allowance provides sufficient time to collect and process all necessary data after stable plant conditions are established. The 30 day Completion Time recognizes at least one other form of leakage detection is available.

[C.1 and C.2

If the required containment air cooler condensate flow rate monitor is inoperable, alternative action is again required. Either SR 3.4.15.1 must be performed, or water inventory balances, in accordance with SR 3.4.13.1, must be performed to provide alternate periodic information. Provided a CHANNEL CHECK is performed every 8 hours or an inventory balance is performed every 24 hours, reactor operation may continue while awaiting restoration of the containment air cooler condensate flow rate monitor to OPERABLE status.

The 24 hour interval provides periodic information that is adequate to detect RCS LEAKAGE. A Note is added allowing that SR 3.4.13.1 is not required to be performed until 12 hours after establishing steady state operation (stable temperature, power level, pressurizer and makeup tank levels, makeup and letdown, and [RCP seal injection and return flows]). The 12 hour allowance provides sufficient time to collect and process all necessary data after stable plant conditions are established.

BASES

ACTIONS (continued)

D.1 and D.2

If the required containment atmosphere radioactivity monitor and the containment air cooler condensate flow rate monitor are inoperable, the only means of detecting leakage is the containment sump monitor. This Condition does not provide the required diverse means of leakage detection. The Required Action is to restore either of the inoperable monitors to OPERABLE status within 30 days to regain the intended leakage detection diversity. The 30 day Completion Times ensure that the plant will not be operated in a reduced configuration for a lengthy time period.]

E.1 and E.2

If any Required Action of Condition A, B, [C], or [D] cannot be met within the required Completion Time, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 5 within 36 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

F.1

If all required monitors are inoperable, no automatic means of monitoring leakage are available and immediate plant shutdown in accordance with LCO 3.0.3 is required.

SURVEILLANCE REQUIREMENTS

SR 3.4.15.1

SR 3.4.15.1 requires the performance of a CHANNEL CHECK of the required containment atmosphere radioactivity monitors. The check gives reasonable confidence the channel is operating properly. The Frequency of [12] hours is based on instrument reliability and is reasonable for detecting off normal conditions.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.4.15.2

SR 3.4.15.2 requires the performance of a CHANNEL FUNCTIONAL TEST of the required containment atmosphere radioactivity monitors. The test ensures that the monitor can perform its function in the desired manner. The test verifies the alarm setpoint and relative accuracy of the instrument string. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions. The Frequency of 92 days considers instrument reliability, and operating experience has shown it proper for detecting degradation.

SR 3.4.15.3, SR 3.4.15.4, and [SR 3.4.15.5]

These SRs require the performance of a CHANNEL CALIBRATION for each of the RCS leakage detection instrumentation channels. The calibration verifies the accuracy of the instrument string, including the instruments located inside containment. The Frequency of [18] months is a typical refueling cycle and considers channel reliability. Operating experience has shown this Frequency is acceptable.

REFERENCES

1. 10 CFR 50, Appendix A, Section IV, GDC 30.
2. Regulatory Guide 1.45.
3. FSAR, Section [ ].

B 3.4 REACTOR COOLANT SYSTEM (RCS)

B 3.4.16 RCS Specific Activity

BASES

BACKGROUND

The Code of Federal Regulations, 10 CFR 100 (Ref. 1) specifies the maximum dose to the whole body and the thyroid an individual at the site boundary can receive for 2 hours during an accident. The limits on specific activity ensure that the doses are held to a small fraction of the 10 CFR 100 limits during analyzed transients and accidents.

The RCS specific activity LCO limits the allowable concentration level of radionuclides in the reactor coolant. The LCO limits are established to minimize the offsite radioactivity dose consequences in the event of a steam generator tube rupture (SGTR) accident.

The LCO contains specific activity limits for both DOSE EQUIVALENT I-131 and gross specific activity. The allowable levels are intended to limit the 2 hour dose at the site boundary to a small fraction of the 10 CFR 100 dose guideline limits. The limits in the LCO are standardized based on parametric evaluations of offsite radioactivity dose consequences for typical site locations.

The parametric evaluations showed the potential offsite dose levels for an SGTR accident were an appropriately small fraction of the 10 CFR 100 dose guideline limits. Each evaluation assumes a broad range of site applicable atmospheric dispersion factors in a parametric evaluation.

APPLICABLE SAFETY ANALYSES

The LCO limits on the specific activity of the reactor coolant ensure that the resulting 2 hour doses at the site boundary will not exceed a small fraction of the 10 CFR 100 dose guideline limits following an SGTR accident. The SGTR safety analysis (Ref. 2) assumes the specific activity of the reactor coolant at the LCO limits and an existing reactor coolant steam generator (SG) tube leakage rate of 1 gpm. The analysis also assumes a reactor trip and a turbine trip at the same time as the SGTR event.

The analysis for the SGTR accident establishes the acceptance limits for RCS specific activity. Reference to this analysis is used to assess changes to the facility that could affect RCS specific activity as they relate to the acceptance limits.

BASES

APPLICABLE SAFETY ANALYSES (continued)

The rise in pressure in the ruptured SG causes radioactively contaminated steam to discharge to the atmosphere through the atmospheric dump valves or the main steam safety valves. The atmospheric discharge stops when the turbine bypass to the condenser removes the excess energy to rapidly reduce the RCS pressure and close the valves. The unaffected SG removes core decay heat by venting steam until the cooldown ends.

The safety analysis shows the radiological consequences of an SGTR accident are within a small fraction of the Reference 1 dose guideline limits. Operation with iodine specific activity levels greater than the LCO limit is permissible, if the activity levels do not exceed the limits shown in Figure 3.4.16-1 for more than 48 hours.

The remainder of the above limit permissible iodine levels shown in Figure 3.4.16-1 are acceptable because of the low probability of an SGTR accident occurring during the established 48 hour time limit. The occurrence of an SGTR accident at these permissible levels could increase the site boundary dose levels, but still be within 10 CFR 100 dose guideline limits.

RCS specific activity satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

The specific iodine activity is limited to 1.0 μCi/gm DOSE EQUIVALENT I-131, and the gross specific activity in the primary coolant is limited to the number of μCi/gm equal to 100 divided by $\bar{E}$ (average disintegration energy of the sum of the average beta and gamma energies of the coolant nuclides). The limit on DOSE EQUIVALENT I-131 ensures the 2 hour thyroid dose to an individual at the site boundary during the Design Basis Accident (DBA) will be a small fraction of the allowed thyroid dose. The limit on gross specific activity ensures the 2 hour whole body dose to an individual at the site boundary during the DBA will be a small fraction of the allowed whole body dose.

The SGTR accident analysis (Ref. 2) shows that the 2 hour site boundary dose levels are within acceptable limits. Violation of the LCO may result in reactor coolant radioactivity levels that could, in the event of an SGTR, lead to site boundary doses that exceed the 10 CFR 100 dose guideline limits.

BASES

APPLICABILITY

In MODES 1 and 2, and in MODE 3 with RCS average temperature ≥ 500°F, operation within the LCO limits for DOSE EQUIVALENT I-131 and gross specific activity is necessary to contain the potential consequences of an SGTR to within the acceptable site boundary dose values.

For operation in MODE 3 with RCS average temperature < 500°F, and in MODES 4 and 5, the release of radioactivity in the event of an SGTR is unlikely since the saturation pressure of the reactor coolant is below the lift pressure settings of the atmospheric dump valves and main steam safety valves.

ACTIONS

A.1 and A.2

With the DOSE EQUIVALENT I-131 greater than the LCO limit, samples at intervals of 4 hours must be taken to demonstrate the limits of Figure 3.4.16-1 are not exceeded. The Completion Time of 4 hours is required to obtain and analyze a sample.

Sampling must continue for trending. The DOSE EQUIVALENT I-131 must be restored to within limits within 48 hours.

The Completion Time of 48 hours is required if the limit violation resulted from normal iodine spiking.

A Note permits the use of the provisions of LCO 3.0.4.c. This allowance permits entry into the applicable MODE(S) while relying on the ACTIONS. This allowance is acceptable due to the significant conservatism incorporated into the specific activity limit, the low probability of an event which is limiting due to exceeding this limit, and the ability to restore transient specific activity excursions while the plant remains at, or proceeds to power operation.

B.1

If a Required Action and associated Completion Time of Condition A is not met or if the DOSE EQUIVALENT I-131 is in the unacceptable region of Figure 3.4.16-1, the reactor must be brought to MODE 3 with RCS average temperature < 500°F within 6 hours. The allowed Completion Time of 6 hours is required to reach MODE 3 below 500°F without challenging plant systems.

BASES

ACTIONS (continued)

C.1

With the gross specific activity in excess of the allowed limit, the unit must be placed in a MODE in which the requirement does not apply.

The change within 6 hours to MODE 3 and RCS average temperature < 500°F lowers the saturation pressure of the reactor coolant below the setpoints of the main steam safety valves and prevents venting the SG to the environment in an SGTR event. The allowed Completion Time of 6 hours is required to reach MODE 3 below 500°F from full power conditions and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.4.16.1

The Surveillance requires performing a gamma isotopic analysis as a measure of the gross specific activity of the reactor coolant at least once per 7 days. While basically a quantitative measure of radionuclides with half lives longer than 15 minutes, excluding iodines, this measurement is the sum of the degassed gamma activities and the gaseous gamma activities in the sample taken. This Surveillance provides an indication of any increase in gross specific activity.

Trending the results of this Surveillance allows proper remedial action to be taken before reaching the LCO limit under normal operating conditions. The Surveillance is applicable in MODES 1 and 2, and in MODE 3 with RCS average temperature at least 500°F. The 7 day Frequency considers the unlikelihood of a gross fuel failure during the time.

SR 3.4.16.2

This Surveillance is performed to ensure iodine remains within limit during normal operation and following fast power changes when fuel failure is more apt to occur. The 14 day Frequency is adequate to trend changes in the iodine activity level considering gross activity is monitored every 7 days. The Frequency, between 2 hours and 6 hours after a power change of ≥ 15% RTP within a 1 hour period, is established because the iodine levels peak during this time following fuel failure; samples at other times would provide inaccurate results.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.4.16.3

A radiochemical analysis for Ē determination is required every 184 days (6 months) with the plant operating in MODE 1 equilibrium conditions. The Ē determination directly relates to the LCO and is required to verify plant operation within the specified gross activity LCO limit. The analysis for Ē is a measurement of the average energies per disintegration for isotopes with half lives longer than 15 minutes, excluding iodines. The Frequency of 184 days recognizes Ē does not change rapidly.

This SR has been modified by a Note that indicates sampling is required to be performed within 31 days after 2 effective full power days and 20 days of MODE 1 operation have elapsed since the reactor was last subcritical for at least 48 hours. This ensures the radioactive materials are at equilibrium so the analysis for Ē is representative and not skewed by a crud burst or other similar abnormal event.

REFERENCES

1. 10 CFR 100.11, 1973.

2. FSAR, Section [15.6.3].

B 3.4 REACTOR COOLANT SYSTEM (RCS)

B 3.4.17 Special Test Exception (STE) RCS Loops

BASES

BACKGROUND	This special test exception to LCO 3.4.4, "RCS Loops - MODES 1 and 2," and LCO 3.3.1, "RPS Instrumentation," permits reactor criticality under no flow conditions during PHYSICS TESTS (natural circulation demonstration, station blackout, and loss of offsite power) while at low THERMAL POWER levels. Section XI of 10 CFR Part 50, Appendix B (Ref. 1), requires that a test program be established to ensure that structures, systems, and components will perform satisfactorily in service. All functions necessary to ensure that the specified design conditions are not exceeded during normal operation and anticipated operational occurrences must be tested. This testing is an integral part of the design, construction, and operation of the power plant as specified in 10 CFR 50, Appendix A, GDC 1 (Ref. 2). The key objectives of a test program are to provide assurance that the facility has been adequately designed to validate the analytical models used in the design and analysis, to verify the assumptions used to predict plant response, to provide assurance that installation of equipment at the facility has been accomplished in accordance with the design, and to verify that the operating and emergency procedures are adequate. Testing is performed prior to initial criticality, during startup, and following low power operations. The tests will include verifying the ability to establish and maintain natural circulation following a plant trip between 10% and 20% RTP, performing natural circulation cooldown on emergency power, and during the cooldown, showing that adequate boron mixing occurs and that pressure can be controlled using auxiliary spray and pressurizer heaters powered from the emergency power sources.
APPLICABLE SAFETY ANALYSES	As described in LCO 3.0.7, compliance with Special Test Exception LCOs is optional, and therefore no criteria of 10 CFR 50.36(c)(2)(ii) apply. Special Test Exception LCOs provide flexibility to perform certain operations by appropriately modifying requirements of other LCOs. A discussion of the criteria satisfied for the other LCOs is provided in their respective Bases.

BASES

LCO

This LCO is provided to allow for the performance of PHYSICS TESTS in MODE 2 (after a refueling), where the core cooling requirements are significantly different than after the core has been operating. Without this LCO, plant operations would be held bound to the normal operating LCOs for reactor coolant loops and circulation (MODES 1 and 2), and the appropriate tests could not be performed.

In MODE 2, where core power level is considerably lower and the associated PHYSICS TESTS must be performed, operation is allowed under no flow conditions provided THERMAL POWER is < 5% RTP and the reactor trip setpoints of the OPERABLE power level channels are set ≤ 20% RTP. These limits ensure no Safety Limits or fuel design limits will be violated.

The exception is allowed even though there are no bounding safety analyses. These tests are allowed since they are performed under close supervision during the test program and provide valuable information on the plant's capability to cool down without offsite power available to the reactor coolant pumps.

APPLICABILITY

This LCO ensures that the plant will not be operated in MODE 1 without forced circulation. It only allows testing under these conditions while in MODE 2. This testing establishes that heat input from nuclear heat does not exceed the natural circulation heat removal capabilities. Therefore, no safety or fuel design limits will be violated as a result of the associated tests.

ACTIONS

A.1

If THERMAL POWER increases to > 5% RTP, the reactor must be tripped immediately. This ensures the plant is not placed in an unanalyzed condition and prevents exceeding the specified acceptable fuel design limits.

SURVEILLANCE REQUIREMENTS

SR 3.4.17.1

THERMAL POWER must be verified to be within limits once per hour to ensure that the fuel design criteria are not violated during the performance of the PHYSICS TESTS. The hourly Frequency has been shown by operating practice to be sufficient to regularly assess conditions for potential degradation and verify operation is within the LCO limits. Plant operations are conducted slowly during the performance of PHYSICS TESTS, and monitoring the power level once per hour is sufficient to ensure that the power level does not exceed the limit.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.4.17.2

Within 12 hours of initiating startup or PHYSICS TESTS, a CHANNEL FUNCTIONAL TEST must be performed on each logarithmic power level and linear power level neutron flux monitoring channel to verify OPERABILITY and adjust setpoints to proper values. This will ensure that the Reactor Protection System is properly aligned to provide the required degree of core protection during startup or the performance of the PHYSICS TESTS. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions. The interval is adequate to ensure that the appropriate equipment is OPERABLE prior to the tests to aid the monitoring and protection of the plant during these tests.

REFERENCES

1. 10 CFR 50, Appendix B, Section XI.
2. 10 CFR 50, Appendix A, GDC 1, 1988.

B 3.4 REACTOR COOLANT SYSTEM (RCS)

B 3.4.18 Steam Generator (SG) Tube Integrity

BASES

BACKGROUND

Steam generator (SG) tubes are small diameter, thin walled tubes that carry primary coolant through the primary to secondary heat exchangers. The SG tubes have a number of important safety functions. Steam generator tubes are an integral part of the reactor coolant pressure boundary (RCPB) and, as such, are relied on to maintain the primary system's pressure and inventory. The SG tubes isolate the radioactive fission products in the primary coolant from the secondary system. In addition, as part of the RCPB, the SG tubes are unique in that they act as the heat transfer surface between the primary and secondary systems to remove heat from the primary system. This Specification addresses only the RCPB integrity function of the SG. The SG heat removal function is addressed by LCO 3.4.4, "RCS Loops – MODES 1 and 2," LCO 3.4.5, "RCS Loops – MODE 3," LCO 3.4.6, "RCS Loops – MODE 4," and LCO 3.4.7, "RCS Loops – MODE 5, Loops Filled.

SG tube integrity means that the tubes are capable of performing their intended RCPB safety function consistent with the licensing basis, including applicable regulatory requirements.

Steam generator tubing is subject to a variety of degradation mechanisms. Steam generator tubes may experience tube degradation related to corrosion phenomena, such as wastage, pitting, intergranular attack, and stress corrosion cracking, along with other mechanically induced phenomena such as denting and wear. These degradation mechanisms can impair tube integrity if they are not managed effectively. The SG performance criteria are used to manage SG tube degradation.

Specification 5.5.9, "Steam Generator (SG) Program," requires that a program be established and implemented to ensure that SG tube integrity is maintained. Pursuant to Specification 5.5.9, tube integrity is maintained when the SG performance criteria are met. There are three SG performance criteria: structural integrity, accident induced leakage, and operational LEAKAGE. The SG performance criteria are described in Specification 5.5.9. Meeting the SG performance criteria provides reasonable assurance of maintaining tube integrity at normal and accident conditions.

The processes used to meet the SG performance criteria are defined by the Steam Generator Program Guidelines (Ref. 1).

BASES

APPLICABLE SAFETY ANALYSES

The steam generator tube rupture (SGTR) accident is the limiting design basis event for SG tubes and avoiding an SGTR is the basis for this Specification. The analysis of a SGTR event assumes a bounding primary to secondary LEAKAGE rate equal to the operational LEAKAGE rate limits in LCO 3.4.13, "RCS Operational LEAKAGE," plus the leakage rate associated with a double-ended rupture of a single tube. The accident analysis for a SGTR assumes the contaminated secondary fluid is only briefly released to the atmosphere via safety valves and the majority is discharged to the main condenser.

The analysis for design basis accidents and transients other than a SGTR assume the SG tubes retain their structural integrity (i.e., they are assumed not to rupture.) In these analyses, the steam discharge to the atmosphere is based on the total primary to secondary LEAKAGE from all SGs of [1 gallon per minute] or is assumed to increase to [1 gallon per minute] as a result of accident induced conditions. For accidents that do not involve fuel damage, the primary coolant activity level of DOSE EQUIVALENT I-131 is assumed to be equal to the LCO 3.4.16, "RCS Specific Activity," limits. For accidents that assume fuel damage, the primary coolant activity is a function of the amount of activity released from the damaged fuel. The dose consequences of these events are within the limits of GDC 19 (Ref. 2), 10 CFR 100 (Ref. 3) or the NRC approved licensing basis (e.g., a small fraction of these limits).

Steam generator tube integrity satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

The LCO requires that SG tube integrity be maintained. The LCO also requires that all SG tubes that satisfy the repair criteria be plugged [or repaired] in accordance with the Steam Generator Program.

During an SG inspection, any inspected tube that satisfies the Steam Generator Program repair criteria is [repaired or] removed from service by plugging. If a tube was determined to satisfy the repair criteria but was not plugged [or repaired], the tube may still have tube integrity.

In the context of this Specification, a SG tube is defined as the entire length of the tube, including the tube wall [and any repairs made to it], between the tube-to-tubesheet weld at the tube inlet and the tube-to-tubesheet weld at the tube outlet. The tube-to-tubesheet weld is not considered part of the tube.

A SG tube has tube integrity when it satisfies the SG performance criteria. The SG performance criteria are defined in Specification 5.5.9, "Steam Generator Program," and describe acceptable SG tube performance. The Steam Generator Program also provides the evaluation process for determining conformance with the SG performance criteria.

BASES

LCO (continued)

There are three SG performance criteria: structural integrity, accident induced leakage, and operational LEAKAGE. Failure to meet any one of these criteria is considered failure to meet the LCO.

The structural integrity performance criterion provides a margin of safety against tube burst or collapse under normal and accident conditions, and ensures structural integrity of the SG tubes under all anticipated transients included in the design specification. Tube burst is defined as, "The gross structural failure of the tube wall. The condition typically corresponds to an unstable opening displacement (e.g., opening area increased in response to constant pressure) accompanied by ductile (plastic) tearing of the tube material at the ends of the degradation." Tube collapse is defined as, "For the load displacement curve for a given structure, collapse occurs at the top of the load versus displacement curve where the slope of the curve becomes zero." The structural integrity performance criterion provides guidance on assessing loads that have a significant effect on burst or collapse. In that context, the term "significant" is defined as "An accident loading condition other than differential pressure is considered significant when the addition of such loads in the assessment of the structural integrity performance criterion could cause a lower structural limit or limiting burst/collapse condition to be established." For tube integrity evaluations, except for circumferential degradation, axial thermal loads are classified as secondary loads. For circumferential degradation, the classification of axial thermal loads as primary or secondary loads will be evaluated on a case-by-case basis. The division between primary and secondary classifications will be based on detailed analysis and/or testing.

Structural integrity requires that the primary membrane stress intensity in a tube not exceed the yield strength for all ASME Code, Section III, Service Level A (normal operating conditions) and Service Level B (upset or abnormal conditions) transients included in the design specification. This includes safety factors and applicable design basis loads based on ASME Code, Section III, Subsection NB (Ref. 4) and Draft Regulatory Guide 1.121 (Ref. 5).

The accident induced leakage performance criterion ensures that the primary to secondary LEAKAGE caused by a design basis accident, other than a SGTR, is within the accident analysis assumptions. The accident analysis assumes that accident induced leakage does not exceed [1 gpm per SG, except for specific types of degradation at specific locations where the NRC has approved greater accident induced leakage.] The accident induced leakage rate includes any primary to secondary LEAKAGE existing prior to the accident in addition to primary to secondary LEAKAGE induced during the accident.

BASES

LCO (continued)

The operational LEAKAGE performance criterion provides an observable indication of SG tube conditions during plant operation. The limit on operational LEAKAGE is contained in LCO 3.4.13, "RCS Operational LEAKAGE," and limits primary to secondary LEAKAGE through any one SG to 150 gallons per day. This limit is based on the assumption that a single crack leaking this amount would not propagate to a SGTR under the stress conditions of a LOCA or a main steam line break. If this amount of LEAKAGE is due to more than one crack, the cracks are very small, and the above assumption is conservative.

APPLICABILITY

Steam generator tube integrity is challenged when the pressure differential across the tubes is large. Large differential pressures across SG tubes can only be experienced in MODE 1, 2, 3, or 4.

RCS conditions are far less challenging in MODES 5 and 6 than during MODES 1, 2, 3, and 4. In MODES 5 and 6, primary to secondary differential pressure is low, resulting in lower stresses and reduced potential for LEAKAGE.

ACTIONS

The ACTIONS are modified by a Note clarifying that the Conditions may be entered independently for each SG tube. This is acceptable because the Required Actions provide appropriate compensatory actions for each affected SG tube. Complying with the Required Actions may allow for continued operation, and subsequent affected SG tubes are governed by subsequent Condition entry and application of associated Required Actions.

<u>A.1 and A.2</u>

Condition A applies if it is discovered that one or more SG tubes examined in an inservice inspection satisfy the tube repair criteria but were not plugged [or repaired] in accordance with the Steam Generator Program as required by SR 3.4.18.2. An evaluation of SG tube integrity of the affected tube(s) must be made. Steam generator tube integrity is based on meeting the SG performance criteria described in the Steam Generator Program. The SG repair criteria define limits on SG tube degradation that allow for flaw growth between inspections while still providing assurance that the SG performance criteria will continue to be met. In order to determine if a SG tube that should have been plugged [or repaired] has tube integrity, an evaluation must be completed that demonstrates that the SG performance criteria will continue to be met until the next refueling outage or SG tube inspection. The tube integrity

BASES

ACTIONS (continued)

determination is based on the estimated condition of the tube at the time the situation is discovered and the estimated growth of the degradation prior to the next SG tube inspection. If it is determined that tube integrity is not being maintained, Condition B applies.

A Completion Time of 7 days is sufficient to complete the evaluation while minimizing the risk of plant operation with a SG tube that may not have tube integrity.

If the evaluation determines that the affected tube(s) have tube integrity, Required Action A.2 allows plant operation to continue until the next refueling outage or SG inspection provided the inspection interval continues to be supported by an operational assessment that reflects the affected tubes. However, the affected tube(s) must be plugged [or repaired] prior to entering MODE 4 following the next refueling outage or SG inspection. This Completion Time is acceptable since operation until the next inspection is supported by the operational assessment.

B.1 and B.2

If the Required Actions and associated Completion Times of Condition A are not met or if SG tube integrity is not being maintained, the reactor must be brought to MODE 3 within 6 hours and MODE 5 within 36 hours.

The allowed Completion Times are reasonable, based on operating experience, to reach the desired plant conditions from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.4.18.1

During shutdown periods the SGs are inspected as required by this SR and the Steam Generator Program. NEI 97-06, Steam Generator Program Guidelines (Ref. 1), and its referenced EPRI Guidelines, establish the content of the Steam Generator Program. Use of the Steam Generator Program ensures that the inspection is appropriate and consistent with accepted industry practices.

During SG inspections a condition monitoring assessment of the SG tubes is performed. The condition monitoring assessment determines the "as found" condition of the SG tubes. The purpose of the condition monitoring assessment is to ensure that the SG performance criteria have been met for the previous operating period.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The Steam Generator Program determines the scope of the inspection and the methods used to determine whether the tubes contain flaws satisfying the tube repair criteria. Inspection scope (i.e., which tubes or areas of tubing within the SG are to be inspected) is a function of existing and potential degradation locations. The Steam Generator Program also specifies the inspection methods to be used to find potential degradation. Inspection methods are a function of degradation morphology, non-destructive examination (NDE) technique capabilities, and inspection locations.

The Steam Generator Program defines the Frequency of SR 3.4.18.1. The Frequency is determined by the operational assessment and other limits in the SG examination guidelines (Ref. 6). The Steam Generator Program uses information on existing degradations and growth rates to determine an inspection Frequency that provides reasonable assurance that the tubing will meet the SG performance criteria at the next scheduled inspection. In addition, Specification 5.5.9 contains prescriptive requirements concerning inspection intervals to provide added assurance that the SG performance criteria will be met between scheduled inspections.

SR 3.4.18.2

During an SG inspection, any inspected tube that satisfies the Steam Generator Program repair criteria is [repaired or] removed from service by plugging. The tube repair criteria delineated in Specification 5.5.9 are intended to ensure that tubes accepted for continued service satisfy the SG performance criteria with allowance for error in the flaw size measurement and for future flaw growth. In addition, the tube repair criteria, in conjunction with other elements of the Steam Generator Program, ensure that the SG performance criteria will continue to be met until the next inspection of the subject tube(s). Reference 1 provides guidance for performing operational assessments to verify that the tubes remaining in service will continue to meet the SG performance criteria.

[Steam generator tube repairs are only performed using approved repair methods as described in the Steam Generator Program.]

The Frequency of prior to entering MODE 4 following a SG inspection ensures that the Surveillance has been completed and all tubes meeting the repair criteria are plugged [or repaired] prior to subjecting the SG tubes to significant primary to secondary pressure differential.

BASES

REFERENCES

1. NEI 97-06, "Steam Generator Program Guidelines."

2. 10 CFR 50 Appendix A, GDC 19.

3. 10 CFR 100.

4. ASME Boiler and Pressure Vessel Code, Section III, Subsection NB.

5. Draft Regulatory Guide 1.121, "Basis for Plugging Degraded Steam Generator Tubes," August 1976.

6. EPRI, "Pressurized Water Reactor Steam Generator Examination Guidelines."

B 3.5 EMERGENCY CORE COOLING SYSTEMS (ECCS)

B 3.5.1 Safety Injection Tanks (SITs)

BASES

BACKGROUND

The functions of the [four] SITs are to supply water to the reactor vessel during the blowdown phase of a loss of coolant accident (LOCA), to provide inventory to help accomplish the refill phase that follows thereafter, and to provide Reactor Coolant System (RCS) makeup for a small break LOCA.

The blowdown phase of a large break LOCA is the initial period of the transient during which the RCS departs from equilibrium conditions, and heat from fission product decay, hot internals, and the vessel continues to be transferred to the reactor coolant. The blowdown phase of the transient ends when the RCS pressure falls to a value approaching that of the containment atmosphere.

The refill phase of a LOCA follows immediately where reactor coolant inventory has vacated the core through steam flashing and ejection out through the break. The core is essentially in adiabatic heatup. The balance of the SITs' inventory is then available to help fill voids in the lower plenum and reactor vessel downcomer to establish a recovery level at the bottom of the core and ongoing reflood of the core with the addition of safety injection (SI) water.

The SITs are pressure vessels partially filled with borated water and pressurized with nitrogen gas. The SITs are passive components, since no operator or control action is required for them to perform their function. Internal tank pressure is sufficient to discharge the contents to the RCS, if RCS pressure decreases below the SIT pressure.

Each SIT is piped into one RCS cold leg via the injection lines utilized by the High Pressure Safety Injection and Low Pressure Safety Injection (HPSI and LPSI) systems. Each SIT is isolated from the RCS by a motor operated isolation valve and two check valves in series. The motor operated isolation valves are normally open, with power removed from the valve motor to prevent inadvertent closure prior to or during an accident.

The SIT gas and water volumes, gas pressure, and outlet pipe size are selected to allow three of the four SITs to partially recover the core before significant clad melting or zirconium water reaction can occur following a LOCA. The need to ensure that three SITs are adequate for this function is consistent with the LOCA assumption that the entire contents of one SIT will be lost via the break during the blowdown phase of a LOCA.

BASES

APPLICABLE SAFETY ANALYSES

The SITs are taken credit for in both the large and small break LOCA analyses at full power (Ref. 1). These are the Design Basis Accidents (DBAs) that establish the acceptance limits for the SITs. Reference to the analyses for these DBAs is used to assess changes to the SITs as they relate to the acceptance limits.

In performing the LOCA calculations, conservative assumptions are made concerning the availability of SI flow. These assumptions include signal generation time, equipment starting times, and delivery time due to system piping. In the early stages of a LOCA with a loss of offsite power, the SITs provide the sole source of makeup water to the RCS. (The assumption of a loss of offsite power is required by regulations.) This is because the LPSI pumps, HPSI pumps, and charging pumps cannot deliver flow until the diesel generators (DGs) start, come to rated speed, and go through their timed loading sequence. In cold leg breaks, the entire contents of one SIT are assumed to be lost through the break during the blowdown and reflood phases.

The limiting large break LOCA is a double ended guillotine cold leg break at the discharge of the reactor coolant pump.

During this event, the SITs discharge to the RCS as soon as RCS pressure decreases to below SIT pressure. As a conservative estimate, no credit is taken for SI pump flow until the SITs are empty. This results in a minimum effective delay of over 60 seconds, during which the SITs must provide the core cooling function. The actual delay time does not exceed 30 seconds. No operator action is assumed during the blowdown stage of a large break LOCA.

The worst case small break LOCA also assumes a time delay before pumped flow reaches the core. For the larger range of small breaks, the rate of blowdown is such that the increase in fuel clad temperature is terminated solely by the SITs, with pumped flow then providing continued cooling. As break size decreases, the SITs and HPSI pumps both play a part in terminating the rise in clad temperature. As break size continues to decrease, the role of the SITs continues to decrease until they are not required, and the HPSI pumps become solely responsible for terminating the temperature increase.

This LCO helps to ensure that the following acceptance criteria, established by 10 CFR 50.46 (Ref. 2) for the ECCS, will be met following a LOCA:

BASES

APPLICABLE SAFETY ANALYSES (continued)

a. Maximum fuel element cladding temperature is ≤ 2200°F,

b. Maximum cladding oxidation is ≤ 0.17 times the total cladding thickness before oxidation,

c. Maximum hydrogen generation from a zirconium water reaction is ≤ 0.01 times the hypothetical amount that would be generated if all of the metal in the cladding cylinders surrounding the fuel, excluding the cladding surrounding the plenum volume, were to react, and

d. The core is maintained in a coolable geometry.

Since the SITs discharge during the blowdown phase of a LOCA, they do not contribute to the long term cooling requirements of 10 CFR 50.46.

Since the SITs are passive components, single active failures are not applicable to their operation. The SIT isolation valves, however, are not single failure proof; therefore, whenever the valves are open, power is removed from their operators and the switch is key locked open.

These precautions ensure that the SITs are available during an accident (Ref. 3). With power supplied to the valves, a single active failure could result in a valve closure, which would render one SIT unavailable for injection. If a second SIT is lost through the break, only two SITs would reach the core. Since the only active failure that could affect the SITs would be the closure of a motor operated outlet valve, the requirement to remove power from these eliminates this failure mode.

The minimum volume requirement for the SITs ensures that three SITs can provide adequate inventory to reflood the core and downcomer following a LOCA. The downcomer then remains flooded until the HPSI and LPSI systems start to deliver flow.

The maximum volume limit is based on maintaining an adequate gas volume to ensure proper injection and the ability of the SITs to fully discharge, as well as limiting the maximum amount of boron inventory in the SITs.

BASES

APPLICABLE SAFETY ANALYSES (continued)

A minimum of 25% narrow range level, corresponding to [1790] cubic feet of borated water, and a maximum of 75% narrow range level, corresponding to [1927] cubic feet of borated water, are used in the safety analyses as the volume in the SITs. To allow for instrument inaccuracy, a [28]% narrow range (corresponding to [1802] cubic feet) and a [72]% narrow range (corresponding to [1914] cubic feet) are specified. The analyses are based upon the cubic feet requirements; the percentage figures are provided for operator use because the level indicator provided in the control room is marked in percentages, not in cubic feet.

The minimum nitrogen cover pressure requirement ensures that the contained gas volume will generate discharge flow rates during injection that are consistent with those assumed in the safety analyses.

The maximum nitrogen cover pressure limit ensures that excessive amounts of gas will not be injected into the RCS after the SITs have emptied.

A minimum pressure of [593] psig and a maximum pressure of [632] psig are used in the analyses. To allow for instrument accuracy, a [615] psig minimum and [655] psig maximum are specified. The maximum allowable boron concentration of [2800] ppm is based upon boron precipitation limits in the core following a LOCA. Establishing a maximum limit for boron is necessary since the time at which boron precipitation would occur in the core following a LOCA is a function of break location, break size, the amount of boron injected into the core, and the point of ECCS injection. Post LOCA emergency procedures directing the operator to establish simultaneous hot and cold leg injection are based on the worst case minimum boron precipitation time. Maintaining the maximum SIT boron concentration within the upper limit ensures that the SITs do not invalidate this calculation. An excessive boron concentration in any of the borated water sources used for injection during a LOCA could result in boron precipitation earlier than predicted.

The minimum boron requirements of [1500] ppm are based on beginning of life reactivity values and are selected to ensure that the reactor will remain subcritical during the reflood stage of a large break LOCA. During a large break LOCA, all control element assemblies (CEAs) are assumed not to insert into the core, and the initial reactor shutdown is

BASES

APPLICABLE SAFETY ANALYSES (continued)

accomplished by void formation during blowdown. Sufficient boron concentration must be maintained in the SITs to prevent a return to criticality during reflood. Although this requirement is similar to the basis for the minimum boron concentration of the refueling water tank (RWT), the minimum SIT concentration is lower than that of the RWT since the SITs need not account for dilution by the RCS.

The SITs satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

The LCO establishes the minimum conditions required to ensure that the SITs are available to accomplish their core cooling safety function following a LOCA. [Four] SITs are required to be OPERABLE to ensure that 100% of the contents of [three] of the SITs will reach the core during a LOCA.

This is consistent with the assumption that the contents of one tank spill through the break. If the contents of fewer than three tanks are injected during the blowdown phase of a LOCA, the ECCS acceptance criteria of 10 CFR 50.46 (Ref. 2) could be violated.

For an SIT to be considered OPERABLE, the isolation valve must be fully open, power removed above [2000] psig, and the limits established in the SR for contained volume, boron concentration, and nitrogen cover pressure must be met.

APPLICABILITY

In MODES 1 and 2, and MODE 3 with RCS pressure ≥ 700 psia, the SIT OPERABILITY requirements are based on an assumption of full power operation. Although cooling requirements decrease as power decreases, the SITs are still required to provide core cooling as long as elevated RCS pressures and temperatures exist.

This LCO is only applicable at pressures ≥ 700 psia. Below 700 psia, the rate of RCS blowdown is such that the ECCS pumps can provide adequate injection to ensure that peak clad temperature remains below the 10 CFR 50.46 (Ref. 2) limit of 2200°F.

In MODE 3, at pressures < 700 psia, and in MODES 4, 5, and 6, the SIT motor operated isolation valves are closed to isolate the SITs from the RCS. This allows RCS cooldown and depressurization without discharging the SITs into the RCS or requiring depressurization of the SITs.

BASES

ACTIONS

A.1

If the boron concentration of one SIT is not within limits, it must be returned to within the limits within 72 hours. In this condition, ability to maintain subcriticality or minimum boron precipitation time may be reduced, but the reduced concentration effects on core subcriticality during reflood are minor. Boiling of the ECCS water in the core during reflood concentrates the boron in the saturated liquid that remains in the core. In addition, the volume of the SIT is still available for injection. Since the boron requirements are based on the average boron concentration of the total volume of three SITs, the consequences are less severe than they would be if an SIT were not available for injection. Thus, 72 hours is allowed to return the boron concentration to within limits.

The combination of redundant level and pressure instrumentation for any single SIT provides sufficient information so that it is not worthwhile to always attempt to correct drift associated with one instrument, with the resulting radiation exposures during entry into containment, as there is sufficient time to repair one in the event that a second one became inoperable. Because these instruments do not initiate a safety action, it is reasonable to extend the allowable outage time for them. While technically inoperable, the SIT will be available to fulfill its safety function during this time and, thus, this Completion Time results in a negligible increase in risk.

B.1

If one SIT is inoperable, for reasons other than boron concentration or the inability to verify level or pressure, the SIT must be returned to OPERABLE status within 24 hours. In this Condition, the required contents of three SITs cannot be assumed to reach the core during a LOCA as is assumed in Appendix K (Ref. 5).

CE NPSD-994 (Ref. 6) provides a series of deterministic and probabilistic findings that support the 24 hour Completion Time as having no affect on risk as compared to shorter periods for restoring the SIT to OPERABLE status.

BASES

ACTIONS (continued)

C.1 and C.2

If the SIT cannot be restored to OPERABLE status within the associated Completion Time, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and pressurizer pressure reduced to < 700 psia within 12 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

D.1

If more than one SIT is inoperable, the unit is in a condition outside the accident analyses. Therefore, LCO 3.0.3 must be entered immediately.

SURVEILLANCE REQUIREMENTS

SR 3.5.1.1

Verification every 12 hours that each SIT isolation valve is fully open, as indicated in the control room, ensures that SITs are available for injection and ensures timely discovery if a valve should be partially closed. If an isolation valve is not fully open, the rate of injection to the RCS would be reduced. Although a motor operated valve should not change position with power removed, a closed valve could result in not meeting accident analysis assumptions. A 12 hour Frequency is considered reasonable in view of other administrative controls that ensure the unlikelihood of a mispositioned isolation valve.

SR 3.5.1.2 and SR 3.5.1.3

SIT borated water volume and nitrogen cover pressure should be verified to be within specified limits every 12 hours in order to ensure adequate injection during a LOCA. Due to the static design of the SITs, a 12 hour Frequency usually allows the operator sufficient time to identify changes before the limits are reached. Operating experience has shown this Frequency to be appropriate for early detection and correction of off normal trends.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.5.1.4

Thirty-one days is reasonable for verification to determine that each SIT's boron concentration is within the required limits, because the static design of the SITs limits the ways in which the concentration can be changed. The 31 day Frequency is adequate to identify changes that could occur from mechanisms such as stratification or inleakage. Sampling the affected SIT within 6 hours after a 1% volume increase will identify whether inleakage has caused a reduction in boron concentration to below the required limit. It is not necessary to verify boron concentration if the added water is from the RWT, because the water contained in the RWT is within the SIT boron concentration requirements. This is consistent with the recommendations of NUREG-1366 (Ref. 4).

SR 3.5.1.5

Verification every 31 days that power is removed from each SIT isolation valve operator when the pressurizer pressure is ≥ 2000 psia ensures that an active failure could not result in the undetected closure of an SIT motor operated isolation valve. If this were to occur, only two SITs would be available for injection, given a single failure coincident with a LOCA. Since installation and removal of power to the SIT isolation valve operators is conducted under administrative control, the 31 day Frequency was chosen to provide additional assurance that power is removed.

This SR allows power to be supplied to the motor operated isolation valves when RCS pressure is < 2000 psia, thus allowing operational flexibility by avoiding unnecessary delays to manipulate the breakers during unit startups or shutdowns.

REFERENCES

1. FSAR, Section [6.3].
2. 10 CFR 50.46.
3. FSAR, Chapter [15].
4. Draft NUREG-1366, February 1990.
5. 10 CFR 50 Appendix K.
6. CE NPSD-994, "CEOG Joint Applications Report for Safety Injection Tank AOT/STI Extension," May 1995.

B 3.5 EMERGENCY CORE COOLING SYSTEMS (ECCS)

B 3.5.2 ECCS - Operating

BASES

BACKGROUND

The function of the ECCS is to provide core cooling and negative reactivity to ensure that the reactor core is protected after any of the following accidents:

a. Loss of coolant accident (LOCA),

b. Control Element Assembly (CEA) ejection accident,

c. Loss of secondary coolant accident, including uncontrolled steam release or loss of feedwater, and

d. Steam generator tube rupture (SGTR).

The addition of negative reactivity is designed primarily for the loss of secondary coolant accident where primary cooldown could add enough positive reactivity to achieve criticality and return to significant power.

There are two phases of ECCS operation: injection and recirculation. In the injection phase, all injection is initially added to the Reactor Coolant System (RCS) via the cold legs. After the blowdown stage of the LOCA stabilizes, injection flow is split equally between the hot and cold legs. After the refueling water tank (RWT) has been depleted, the ECCS recirculation phase is entered as the ECCS suction is automatically transferred to the containment sump.

Two redundant, 100% capacity trains are provided. In MODES 1, 2, and 3, with pressurizer pressure ≥ 1700 psia, each train consists of high pressure safety injection (HPSI), low pressure safety injection (LPSI), and charging subsystems. In MODES 1, 2, and 3, with pressurizer pressure ≥ 1700 psia, both trains must be OPERABLE. This ensures that 100% of the core cooling requirements can be provided in the event of a single active failure.

A suction header supplies water from the RWT or the containment sump to the ECCS pumps. Separate piping supplies each train. The discharge headers from each HPSI pump divide into four supply lines. Both HPSI trains feed into each of the four injection lines. The discharge header from each LPSI pump divides into two supply lines, each feeding the injection line to two RCS cold legs. Control valves or orifices are set to balance the flow to the RCS. This flow balance directs sufficient flow to the core to meet the analysis assumptions following a LOCA in one of the RCS cold legs.

BASES

BACKGROUND (continued)

For LOCAs that are too small to initially depressurize the RCS below the shutoff head of the HPSI pumps, the charging pumps supply water to maintain inventory until the RCS pressure decreases below the HPSI pump shutoff head. During this period, the steam generators (SGs) must provide the core cooling function. The charging pumps take suction from the RWT on a safety injection actuation signal (SIAS) and discharge directly to the RCS through a common header. The normal supply source for the charging pumps is isolated on an SIAS to prevent noncondensible gas (e.g., air, nitrogen, or hydrogen) from being entrained in the charging pumps.

During low temperature conditions in the RCS, limitations are placed on the maximum number of HPSI pumps that may be OPERABLE. Refer to the Bases for LCO 3.4.12, "Low Temperature Overpressure Protection (LTOP) System," for the basis of these requirements.

During a large break LOCA, RCS pressure will decrease to < 200 psia in < 20 seconds. The safety injection (SI) systems are actuated upon receipt of an SIAS. The actuation of safeguard loads is accomplished in a programmed time sequence. If offsite power is available, the safeguard loads start immediately in the programmed sequence. If offsite power is not available, the Engineered Safety Feature (ESF) buses shed normal operating loads and are connected to the diesel generators (DGs). Safeguard loads are then actuated in the programmed time sequence. The time delay associated with diesel starting, sequenced loading, and pump starting determines the time required before pumped flow is available to the core following a LOCA.

The active ECCS components, along with the passive safety injection tanks (SITs) and the RWT, covered in LCO 3.5.1, "Safety Injection Tanks (SITs)," and LCO 3.5.4, "Refueling Water Tank (RWT)," provide the cooling water necessary to meet GDC 35 (Ref. 1).

APPLICABLE SAFETY ANALYSES

The LCO helps to ensure that the following acceptance criteria, established by 10 CFR 50.46 (Ref. 2) for ECCSs, will be met following a LOCA:

a. Maximum fuel element cladding temperature is ≤ 2200°F,

b. Maximum cladding oxidation is ≤ 0.17 times the total cladding thickness before oxidation,

BASES

APPLICABLE SAFETY ANALYSES (continued)

c. Maximum hydrogen generation from a zirconium water reaction is ≤ 0.01 times the hypothetical amount generated if all of the metal in the cladding cylinders surrounding the fuel, excluding the cladding surrounding the plenum volume, were to react,

d. Core is maintained in a coolable geometry, and

e. Adequate long term core cooling capability is maintained.

The LCO also limits the potential for a post trip return to power following a steam line break (SLB) and ensures that containment temperature limits are met.

Both HPSI and LPSI subsystems are assumed to be OPERABLE in the large break LOCA analysis at full power (Ref. 3). This analysis establishes a minimum required runout flow for the HPSI and LPSI pumps, as well as the maximum required response time for their actuation. The HPSI pumps and charging pumps are credited in the small break LOCA analysis. This analysis establishes the flow and discharge head requirements at the design point for the HPSI pump. The SGTR and SLB analyses also credit the HPSI pumps, but are not limiting in their design.

The large break LOCA event with a loss of offsite power and a single failure (disabling one ECCS train) establishes the OPERABILITY requirements for the ECCS. During the blowdown stage of a LOCA, the RCS depressurizes as primary coolant is ejected through the break into the containment. The nuclear reaction is terminated either by moderator voiding during large breaks or control element assembly (CEA) insertion during small breaks. Following depressurization, emergency cooling water is injected into the cold legs, flows into the downcomer, fills the lower plenum, and refloods the core.

On smaller breaks, RCS pressure will stabilize at a value dependent upon break size, heat load, and injection flow. The smaller the break, the higher this equilibrium pressure. In all LOCA analyses, injection flow is not credited until RCS pressure drops below the shutoff head of the HPSI pumps.

BASES

APPLICABLE SAFETY ANALYSES (continued)

The LCO ensures that an ECCS train will deliver sufficient water to match decay heat boiloff rates soon enough to minimize core uncovery for a large LOCA. It also ensures that the HPSI pump will deliver sufficient water during a small break LOCA and provide sufficient boron to maintain the core subcritical following an SLB. For smaller LOCAs, the charging pumps deliver sufficient fluid to maintain RCS inventory until the RCS can be depressurized below the HPSI pumps' shutoff head. During this period of a small break LOCA, the SGs continue to serve as the heat sink providing core cooling.

ECCS - Operating satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

In MODES 1, 2, and 3, with pressurizer pressure ≥ 1700 psia, two independent (and redundant) ECCS trains are required to ensure that sufficient ECCS flow is available, assuming there is a single failure affecting either train. Additionally, individual components within the ECCS trains may be called upon to mitigate the consequences of other transients and accidents.

In MODES 1 and 2, and in MODE 3 with pressurizer pressure ≥ 1700 psia, an ECCS train consists of an HPSI subsystem, an LPSI subsystem, and a charging pump.

Each train includes the piping, instruments, and controls to ensure the availability of an OPERABLE flow path capable of taking suction from the RWT on an SIAS and automatically transferring suction to the containment sump upon a recirculation actuation signal (RAS).

During an event requiring ECCS actuation, a flow path is provided to ensure an abundant supply of water from the RWT to the RCS, via the HPSI and LPSI pumps and their respective supply headers, to each of the four cold leg injection nozzles. In the long term, this flow path may be switched to take its supply from the containment sump and to supply part of its flow to the RCS hot legs via the shutdown cooling (SDC) suction nozzles. The charging pump flow path takes suction from the RWT and supplies the RCS via the normal charging lines.

The flow path for each train must maintain its designed independence to ensure that no single failure can disable both ECCS trains.

BASES

APPLICABILITY

In MODES 1 and 2, and in MODE 3 with RCS pressure ≥ 1700 psia, the ECCS OPERABILITY requirements for the limiting Design Basis Accident (DBA) large break LOCA are based on full power operation. Although reduced power would not require the same level of performance, the accident analysis does not provide for reduced cooling requirements in the lower MODES. The HPSI pump performance is based on the small break LOCA, which establishes the pump performance curve and has less dependence on power. The charging pump performance requirements are based on a small break LOCA. The requirements of MODES 2 and 3, with RCS pressure ≥ 1700 psia, are bounded by the MODE 1 analysis.

The ECCS functional requirements of MODE 3, with RCS pressure < 1700 psia, and MODE 4 are described in LCO 3.5.3, "ECCS - Shutdown."

In MODES 5 and 6, unit conditions are such that the probability of an event requiring ECCS injection is extremely low. Core cooling requirements in MODE 5 are addressed by LCO 3.4.7, "RCS Loops - MODE 5, Loops Filled," and LCO 3.4.8, "RCS Loops - MODE 5, Loops Not Filled." MODE 6 core cooling requirements are addressed by LCO 3.9.4, "Shutdown Cooling (SDC) and Coolant Circulation - High Water Level," and LCO 3.9.5, "Shutdown Cooling (SDC) and Coolant Circulation - Low Water Level."

ACTIONS

A.1

With one LPSI subsystem inoperable, action must be taken to restore OPERABLE status within 7 days. In this condition, the remaining OPERABLE ECCS train is adequate to perform the heat removal function. However, the overall reliability is reduced because a single failure to the remaining LPSI subsystem could result in loss of ECCS function. The 7 day Completion Time is reasonable to perform corrective maintenance on the inoperable LPSI subsystem. The 7 day Completion Time is based on the findings of the deterministic and probabilistic analysis in Reference 6. Reference 6 concluded that extending the Completion Time to 7 days for an inoperable LPSI train provides plant operational flexibility while simultaneously reducing overall plant risk. This is because the risks incurred by having the LPSI train unavailable for a longer time at power will be substantially offset by the benefits associated with avoiding unnecessary plant transitions and by reducing risk during plant shutdown operations.

BASES

ACTIONS (continued)

B.1

If one or more trains are inoperable except for reasons other than Condition A (one LPSI subsystem inoperable) and at least 100% of the ECCS flow equivalent to a single OPERABLE ECCS train is available, the inoperable components must be returned to OPERABLE status within 72 hours. The 72 hour Completion Time is based on an NRC study (Ref. 4) using a reliability evaluation and is a reasonable amount of time to effect many repairs.

An ECCS train is inoperable if it is not capable of delivering the design flow to the RCS. The individual components are inoperable if they are not capable of performing their design function, or if supporting systems are not available.

The LCO requires the OPERABILITY of a number of independent subsystems. Due to the redundancy of trains and the diversity of subsystems, the inoperability of one component in a train does not render the ECCS incapable of performing its function. Neither does the inoperability of two different components, each in a different train, necessarily result in a loss of function for the ECCS. This allows increased flexibility in plant operations when components in opposite trains are inoperable.

An event accompanied by a loss of offsite power and the failure of an emergency DG can disable one ECCS train until power is restored. A reliability analysis (Ref. 4) has shown that the impact with one full ECCS train inoperable is sufficiently small to justify continued operation for 72 hours.

Reference 5 describes situations in which one component, such as a shutdown cooling total flow control valve, can disable both ECCS trains. With one or more components inoperable, such that 100% of the equivalent flow to a single OPERABLE ECCS train is not available, the facility is in a condition outside the accident analyses. Therefore, LCO 3.0.3 must be immediately entered.

BASES

ACTIONS (continued)

C.1 and C.2

If the inoperable train cannot be restored to OPERABLE status within the associated Completion Time, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and pressurizer pressure reduced to < 1700 psia within 12 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required unit conditions from full power in an orderly manner and without challenging unit systems.

D.1

Condition B is applicable with one or more trains inoperable. The allowed Completion Time is based on the assumption that at least 100% of the ECCS flow equivalent to a single OPERABLE ECCS train is available. With less than 100% of the ECCS flow equivalent to a single OPERABLE ECCS train available, the facility is in a condition outside of the accident analyses. Therefore, LCO 3.0.3 must be entered immediately.

SURVEILLANCE REQUIREMENTS

SR 3.5.2.1

Verification of proper valve position ensures that the flow path from the ECCS pumps to the RCS is maintained. Misalignment of these valves could render both ECCS trains inoperable. Securing these valves in position by removing power or by key locking the control in the correct position ensures that the valves cannot be inadvertently misaligned or change position as the result of an active failure. These valves are of the type described in Reference 5, which can disable the function of both ECCS trains and invalidate the accident analysis. A 12 hour Frequency is considered reasonable in view of other administrative controls ensuring that a mispositioned valve is an unlikely possibility.

SR 3.5.2.2

Verifying the correct alignment for manual, power operated, and automatic valves in the ECCS flow paths provides assurance that the proper flow paths will exist for ECCS operation. This SR does not apply to valves that are locked, sealed, or otherwise secured in position, since these valves were verified to be in the correct position prior to locking,

BASES

SURVEILLANCE REQUIREMENTS (continued)

sealing, or securing. A valve that receives an actuation signal is allowed to be in a nonaccident position provided the valve automatically repositions within the proper stroke time. This Surveillance does not require any testing or valve manipulation. Rather, it involves verification that those valves capable of being mispositioned are in the correct position.

The 31 day Frequency is appropriate because the valves are operated under procedural control and an improper valve position would only affect a single train. This Frequency has been shown to be acceptable through operating experience.

SR 3.5.2.3

With the exception of systems in operation, the ECCS pumps are normally in a standby, nonoperating mode. As such, flow path piping has the potential to develop voids and pockets of entrained gases. Maintaining the piping from the ECCS pumps to the RCS full of water ensures that the system will perform properly, injecting its full capacity into the RCS upon demand. This will also prevent water hammer, pump cavitation, and pumping of noncondensible gas (e.g., air, nitrogen, or hydrogen) into the reactor vessel following an SIAS or during SDC. The 31 day Frequency takes into consideration the gradual nature of gas accumulation in the ECCS piping and the adequacy of the procedural controls governing system operation.

SR 3.5.2.4

Periodic surveillance testing of ECCS pumps to detect gross degradation caused by impeller structural damage or other hydraulic component problems is required by the ASME Code. This type of testing may be accomplished by measuring the pump developed head at only one point of the pump characteristic curve. This verifies both that the measured performance is within an acceptable tolerance of the original pump baseline performance and that the performance at the test flow is greater than or equal to the performance assumed in the unit safety analysis. SRs are specified in the Inservice Testing Program of the ASME Code. The ASME Code provides the activities and Frequencies necessary to satisfy the requirements.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.5.2.5

Discharge head at design flow is a normal test of charging pump performance required by the ASME Code. A quarterly Frequency for such tests is a Code requirement. Such inservice inspections detect component degradation and incipient failures.

SR 3.5.2.6, SR 3.5.2.7, and SR 3.5.2.8

These SRs demonstrate that each automatic ECCS valve actuates to the required position on an actual or simulated SIAS and on an RAS, that each ECCS pump starts on receipt of an actual or simulated SIAS, and that the LPSI pumps stop on receipt of an actual or simulated RAS. This Surveillance is not required for valves that are locked, sealed, or otherwise secured in the required position under administrative controls. The 18 month Frequency is based on the need to perform these Surveillances under the conditions that apply during a plant outage and the potential for unplanned transients if the Surveillances were performed with the reactor at power. The 18 month Frequency is also acceptable based on consideration of the design reliability (and confirming operating experience) of the equipment. The actuation logic is tested as part of the Engineered Safety Feature Actuation System (ESFAS) testing, and equipment performance is monitored as part of the Inservice Testing Program.

SR 3.5.2.9

Realignment of valves in the flow path on an SIAS is necessary for proper ECCS performance. The safety injection valves have stops to position them properly so that flow is restricted to a ruptured cold leg, ensuring that the other cold legs receive at least the required minimum flow. This SR is not required for units with flow limiting orifices. The 18 month Frequency is based on the same factors as those stated above for SR 3.5.2.6, SR 3.5.2.7, and SR 3.5.2.8.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.5.2.10

Periodic inspection of the containment sump ensures that it is unrestricted and stays in proper operating condition. The 18 month Frequency is based on the need to perform this Surveillance under the conditions that apply during an outage, on the need to have access to the location, and on the potential for unplanned transients if the Surveillance were performed with the reactor at power. This Frequency is sufficient to detect abnormal degradation and is confirmed by operating experience.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 35.
2. 10 CFR 50.46.
3. FSAR, Chapter [6].
4. NRC Memorandum to V. Stello, Jr., from R. L. Baer, "Recommended Interim Revisions to LCOs for ECCS Components," December 1, 1975.
5. IE Information Notice No. 87-01, January 6, 1987.
6. CE NPSD-995, "Low Pressure Safety Injection System AOT Extension," May 1995.

B 3.5 EMERGENCY CORE COOLING SYSTEMS (ECCS)

B 3.5.3 ECCS - Shutdown

BASES

BACKGROUND	The Background section for Bases B 3.5.2, "ECCS - Operating," is applicable to these Bases, with the following modifications. In MODE 3 with pressurizer pressure < 1700 psia and in MODE 4, an ECCS train is defined as one high pressure safety injection (HPSI) subsystem. The HPSI flow path consists of piping, valves, and pumps that enable water from the refueling water tank (RWT) to be injected into the Reactor Coolant System (RCS) following the accidents described in Bases 3.5.2.
APPLICABLE SAFETY ANALYSES	The Applicable Safety Analyses section of Bases 3.5.2 is applicable to these Bases. Due to the stable conditions associated with operation in MODE 4, and the reduced probability of a Design Basis Accident (DBA), the ECCS operational requirements are reduced. Included in these reductions is that certain automatic safety injection (SI) actuation signals are not available. In this MODE, sufficient time exists for manual actuation of the required ECCS to mitigate the consequences of a DBA. Only one train of ECCS is required for MODE 4. Protection against single failures is not relied on for this MODE of operation. ECCS - Shutdown satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).
LCO	In MODE 3 with pressurizer pressure < 1700 psia, an ECCS subsystem is composed of a single HPSI subsystem. Each HPSI subsystem includes the piping, instruments, and controls to ensure an OPERABLE flow path capable of taking suction from the RWT and transferring suction to the containment sump. During an event requiring ECCS actuation, a flow path is required to supply water from the RWT to the RCS via the HPSI pumps and their respective supply headers to each of the four cold leg injection nozzles. In the long term, this flow path may be switched to take its supply from the containment sump and to deliver its flow to the RCS hot and cold legs.

BASES

LCO (continued)

With RCS pressure < 1700 psia, one HPSI pump is acceptable without single failure consideration, based on the stable reactivity condition of the reactor and the limited core cooling requirements. The low pressure safety injection (LPSI) pumps may therefore be released from the ECCS train for use in shutdown cooling (SDC). In MODE 4 with RCS cold leg temperature less than or equal to the LTOP enable temperature specified in the PTLR, a maximum of one HPSI pump is allowed to be OPERABLE in accordance with LCO 3.4.12, "Low Temperature Overpressure Protection (LTOP) System."

APPLICABILITY

In MODES 1, 2, and 3 with RCS pressure ≥ 1700 psia, the OPERABILITY requirements for ECCS are covered by LCO 3.5.2.

In MODE 3 with RCS pressure < 1700 psia and in MODE 4, one OPERABLE ECCS train is acceptable without single failure consideration, based on the stable reactivity condition of the reactor and the limited core cooling requirements.

In MODES 5 and 6, unit conditions are such that the probability of an event requiring ECCS injection is extremely low. Core cooling requirements in MODE 5 are addressed by LCO 3.4.7, "RCS Loops - MODE 5, Loops Filled," and LCO 3.4.8, "RCS Loops - MODE 5, Loops Not Filled." MODE 6 core cooling requirements are addressed by LCO 3.9.4, "Shutdown Cooling (SDC) and Coolant Circulation - High Water Level," and LCO 3.9.5, "Shutdown Cooling (SDC) and Coolant Circulation - Low Water Level."

ACTIONS

A Note prohibits the application of LCO 3.0.4.b to an inoperable ECCS High Pressure Safety Injection subsystem. There is an increased risk associated with entering MODE 4 from MODE 5 with an inoperable ECCS High Pressure Safety Injection subsystem and the provisions of LCO 3.0.4.b, which allow entry into a MODE or other specified condition in the Applicability with the LCO not met after performance of a risk assessment addressing inoperable systems and components, should not be applied in this circumstance.

A.1

With no HPSI pump OPERABLE, the unit is not prepared to respond to a loss of coolant accident. The 1 hour Completion Time to restore at least one HPSI train to OPERABLE status ensures that prompt action is taken to restore the required cooling capacity or to initiate actions to place the unit in MODE 5, where an ECCS train is not required.

BASES

ACTIONS (continued)

B.1

When the Required Action cannot be completed within the required Completion Time, a controlled shutdown should be initiated. Twenty-four hours is reasonable, based on operating experience, to reach MODE 5 in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.5.3.1

The applicable Surveillance descriptions from Bases 3.5.2 apply.

REFERENCES

The applicable references from Bases 3.5.2 apply.

B 3.5 EMERGENCY CORE COOLING SYSTEMS (ECCS)

B 3.5.4 Refueling Water Tank (RWT)

BASES

BACKGROUND

The RWT supports the ECCS and the Containment Spray System by providing a source of borated water for Engineered Safety Feature (ESF) pump operation.

The RWT supplies two ECCS trains by separate, redundant supply headers. Each header also supplies one train of the Containment Spray System. A motor operated isolation valve is provided in each header to allow the operator to isolate the usable volume of the RWT from the ECCS after the ESF pump suction has been transferred to the containment sump following depletion of the RWT during a loss of coolant accident (LOCA). A separate header is used to supply the Chemical and Volume Control System (CVCS) from the RWT. Use of a single RWT to supply both trains of the ECCS is acceptable since the RWT is a passive component, and passive failures are not assumed to occur coincidently with the Design Basis Event during the injection phase of an accident. Not all the water stored in the RWT is available for injection following a LOCA; the location of the ECCS suction piping in the RWT will result in some portion of the stored volume being unavailable.

The high pressure safety injection (HPSI), low pressure safety injection (LPSI), and containment spray pumps are provided with recirculation lines that ensure each pump can maintain minimum flow requirements when operating at shutoff head conditions. These lines discharge back to the RWT, which vents to the atmosphere. When the suction for the HPSI and containment spray pumps is transferred to the containment sump, this flow path must be isolated to prevent a release of the containment sump contents to the RWT. If not isolated, this flow path could result in a release of contaminants to the atmosphere and the eventual loss of suction head for the ESF pumps.

This LCO ensures that:

a. The RWT contains sufficient borated water to support the ECCS during the injection phase,

b. Sufficient water volume exists in the containment sump to support continued operation of the ESF pumps at the time of transfer to the recirculation mode of cooling, and

c. The reactor remains subcritical following a LOCA.

BASES

BACKGROUND (continued)

Insufficient water inventory in the RWT could result in insufficient cooling capacity of the ECCS when the transfer to the recirculation mode occurs. Improper boron concentrations could result in a reduction of SDM or excessive boric acid precipitation in the core following a LOCA, as well as excessive caustic stress corrosion of mechanical components and systems inside containment.

APPLICABLE SAFETY ANALYSES

During accident conditions, the RWT provides a source of borated water to the HPSI, LPSI, containment spray, and charging pumps. As such, it provides containment cooling and depressurization, core cooling, and replacement inventory and is a source of negative reactivity for reactor shutdown (Ref. 1). The design basis transients and applicable safety analyses concerning each of these systems are discussed in the Applicable Safety Analyses section of Bases B 3.5.2, "ECCS - Operating," and B 3.6.6, "Containment Spray and Cooling Systems." These analyses are used to assess changes to the RWT in order to evaluate their effects in relation to the acceptance limits.

The volume limit of [362,800] gallons is based on two factors:

a. Sufficient deliverable volume must be available to provide at least 20 minutes (plus a 10% margin) of full flow from all ESF pumps prior to reaching a low level switchover to the containment sump for recirculation and

b. The containment sump water volume must be sufficient to support continued ESF pump operation after the switchover to recirculation occurs. This sump volume water inventory is supplied by the RWT borated water inventory.

Twenty minutes is the point at which 75% of the design flow of one HPSI pump is capable of meeting or exceeding the decay heat boiloff rate.

When ESF pump suction is transferred to the sump, there must be sufficient water in the sump to ensure adequate net positive suction head (NPSH) for the HPSI and containment spray pumps. The RWT capacity must be sufficient to supply this amount of water without considering the inventory added from the safety injection tanks or Reactor Coolant System (RCS), but accounting for loss of inventory to containment subcompartments and reservoirs due to containment spray operation and to areas outside containment due to leakage from ECCS injection and recirculation equipment.

BASES

APPLICABLE SAFETY ANALYSES (continued)

The [1720] ppm limit for minimum boron concentration was established to ensure that, following a LOCA with a minimum level in the RWT, the reactor will remain subcritical in the cold condition following mixing of the RWT and RCS water volumes. Small break LOCAs assume that all control rods are inserted, except for the control element assembly (CEA) of highest worth, which is withdrawn from the core. Large break LOCAs assume that all CEAs remain withdrawn from the core. The most limiting case occurs at beginning of core life.

The maximum boron limit of [2500] ppm in the RWT is based on boron precipitation in the core following a LOCA. With the reactor vessel at saturated conditions, the core dissipates heat by pool nucleate boiling. Because of this boiling phenomenon in the core, the boric acid concentration will increase in this region. If allowed to proceed in this manner, a point will be reached where boron precipitation will occur in the core. Post LOCA emergency procedures direct the operator to establish simultaneous hot and cold leg injection to prevent this condition by establishing a forced flow path through the core regardless of break location. These procedures are based on the minimum time in which precipitation could occur, assuming that maximum boron concentrations exist in the borated water sources used for injection following a LOCA. Boron concentrations in the RWT in excess of the limit could result in precipitation earlier than assumed in the analysis.

The upper limit of [100]°F and the lower limit of [40]°F on RWT temperature are the limits assumed in the accident analysis. Although RWT temperature affects the outcome of several analyses, the upper and lower limits established by the LCO are not limited by any of these analyses.

The RWT satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

The RWT ensures that an adequate supply of borated water is available to cool and depressurize the containment in the event of a Design Basis Accident (DBA) and to cool and cover the core in the event of a LOCA, that the reactor remains subcritical following a DBA, and that an adequate level exists in the containment sump to support ESF pump operation in the recirculation mode.

To be considered OPERABLE, the RWT must meet the limits established in the SRs for water volume, boron concentration, and temperature.

BASES

APPLICABILITY

In MODES 1, 2, 3, and 4, the RWT OPERABILITY requirements are dictated by the ECCS and Containment Spray System OPERABILITY requirements. Since both the ECCS and the Containment Spray System must be OPERABLE in MODES 1, 2, 3, and 4, the RWT must be OPERABLE to support their operation.

Core cooling requirements in MODE 5 are addressed by LCO 3.4.7, "RCS Loops - MODE 5, Loops Filled," and LCO 3.4.8, "RCS Loops - MODE 5, Loops Not Filled." MODE 6 core cooling requirements are addressed by LCO 3.9.4, "Shutdown Cooling (SDC) and Coolant Circulation - High Water Level," and LCO 3.9.5, "Shutdown Cooling (SDC) and Coolant Circulation - Low Water Level."

ACTIONS

A.1

With RWT boron concentration or borated water temperature not within limits, it must be returned to within limits within 8 hours. In this condition neither the ECCS nor the Containment Spray System can perform their design functions; therefore, prompt action must be taken to restore the tank to OPERABLE condition. The allowed Completion Time of 8 hours to restore the RWT to within limits was developed considering the time required to change boron concentration or temperature and that the contents of the tank are still available for injection.

B.1

With RWT borated water volume not within limits, it must be returned to within limits within 1 hour. In this condition, neither the ECCS nor Containment Spray System can perform their design functions; therefore, prompt action must be taken to restore the tank to OPERABLE status or to place the unit in a MODE in which these systems are not required. The allowed Completion Time of 1 hour to restore the RWT to OPERABLE status is based on this condition simultaneously affecting multiple redundant trains.

C.1 and C.2

If the RWT cannot be restored to OPERABLE status within the associated Completion Time, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 5 within 36 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.5.4.1

RWT borated water temperature shall be verified every 24 hours to be within the limits assumed in the accident analysis. This Frequency has been shown to be sufficient to identify temperature changes that approach either acceptable limit.

The SR is modified by a Note that eliminates the requirement to perform this Surveillance when ambient air temperatures are within the operating temperature limits of the RWT. With ambient temperatures within this range, the RWT temperature should not exceed the limits.

SR 3.5.4.2

Above minimum RWT water volume level shall be verified every 7 days. This Frequency ensures that a sufficient initial water supply is available for injection and to support continued ESF pump operation on recirculation. Since the RWT volume is normally stable and is provided with a Low Level Alarm, a 7 day Frequency is appropriate and has been shown to be acceptable through operating experience.

SR 3.5.4.3

Boron concentration of the RWT shall be verified every 7 days to be within the required range. This Frequency ensures that the reactor will remain subcritical following a LOCA. Further, it ensures that the resulting sump pH will be maintained in an acceptable range such that boron precipitation in the core will not occur earlier than predicted and the effect of chloride and caustic stress corrosion on mechanical systems and components will be minimized. Since the RWT volume is normally stable, a 7 day sampling Frequency is appropriate and has been shown through operating experience to be acceptable.

REFERENCES

1. FSAR, Chapter [6] and Chapter [15].

B 3.5 EMERGENCY CORE COOLING SYSTEMS (ECCS)

B 3.5.5 Trisodium Phosphate (TSP)

BASES

BACKGROUND

Trisodium phosphate (TSP) is placed on the floor or in the sump of the containment building to ensure that iodine, which may be dissolved in the recirculated reactor cooling water following a loss of coolant accident (LOCA), remains in solution. TSP also helps inhibit stress corrosion cracking (SCC) of austenitic stainless steel components in containment during the recirculation phase following an accident.

Fuel that is damaged during a LOCA will release iodine in several chemical forms to the reactor coolant and to the containment atmosphere. A portion of the iodine in the containment atmosphere is washed to the sump by containment sprays. The emergency core cooling water is borated for reactivity control. This borated water causes the sump solution to be acidic. In a low pH (acidic) solution, dissolved iodine will be converted to a volatile form. The volatile iodine will evolve out of solution into the containment atmosphere, significantly increasing the levels of airborne iodine. The increased levels of airborne iodine in containment contribute to the radiological releases and increase the consequences from the accident due to containment atmosphere leakage.

After a LOCA, the components of the core cooling and containment spray systems will be exposed to high temperature borated water. Prolonged exposure to the core cooling water combined with stresses imposed on the components can cause SCC. The SCC is a function of stress, oxygen and chloride concentrations, pH, temperature, and alloy composition of the components. High temperatures and low pH, which would be present after a LOCA, tend to promote SCC. This can lead to the failure of necessary safety systems or components.

Adjusting the pH of the recirculation solution to levels above 7.0 prevents a significant fraction of the dissolved iodine from converting to a volatile form. The higher pH thus decreases the level of airborne iodine in containment and reduces the radiological consequences from containment atmosphere leakage following a LOCA. Maintaining the solution pH above 7.0 also reduces the occurrence of SCC of austenitic stainless steel components in containment. Reducing SCC reduces the probability of failure of components.

BASES

BACKGROUND (continued)

TSP is employed as a passive form of pH control for post LOCA containment spray and core cooling water. Baskets of TSP are placed on the floor or in the sump of the containment building to dissolve from released reactor coolant water and containment sprays after a LOCA. Recirculation of the water for core cooling and containment sprays then provides mixing to achieve a uniform solution pH. The hydrated form (45-57% moisture) of TSP is used because of the high humidity in the containment building during normal operation. Since the TSP is hydrated, it is less likely to absorb large amounts of water from the humid atmosphere and will undergo less physical and chemical change than the anhydrous form of TSP.

APPLICABLE SAFETY ANALYSES

The LOCA radiological consequences analysis takes credit for iodine retention in the sump solution based on the recirculation water pH being ≥ 7.0. The radionuclide releases from the containment atmosphere and the consequences of a LOCA would be increased if the pH of the recirculation water were not adjusted to 7.0 or above.

TSP satisfies Criterion 3 of the 10 CFR 50.36(c)(2)(ii).

LCO

The TSP is required to adjust the pH of the recirculation water to > 7.0 after a LOCA. A pH > 7.0 is necessary to prevent significant amounts of iodine released from fuel failures and dissolved in the recirculation water from converting to a volatile form and evolving into the containment atmosphere. Higher levels of airborne iodine in containment may increase the release of radionuclides and the consequences of the accident. A pH > 7.0 is also necessary to prevent SCC of austenitic stainless steel components in containment. SCC increases the probability of failure of components.

The required amount of TSP is based upon the extreme cases of water volume and pH possible in the containment sump after a large break LOCA. The minimum required volume is the volume of TSP that will achieve a sump solution pH of ≥ 7.0 when taking into consideration the maximum possible sump water volume and the minimum possible pH. The amount of TSP needed in the containment building is based on the mass of TSP required to achieve the desired pH. However, a required volume is specified, rather than mass, since it is not feasible to weigh the entire amount of TSP in containment. The minimum required volume is based on the manufactured density of TSP. Since TSP can have a tendency to agglomerate from high humidity in the containment building, the density may increase and the volume decrease during normal plant operation. Due to possible agglomeration and increase in density, estimating the minimum volume of TSP in containment is conservative with respect to achieving a minimum required pH.

BASES

APPLICABILITY

In MODES 1, 2, and 3, the RCS is at elevated temperature and pressure, providing an energy potential for a LOCA. The potential for a LOCA results in a need for the ability to control the pH of the recirculated coolant.

In MODES 4, 5, and 6, the potential for a LOCA is reduced or nonexistent, and TSP is not required.

ACTIONS

A.1

If it is discovered that the TSP in the containment building sump is not within limits, action must be taken to restore the TSP to within limits. During plant operation the containment sump is not accessible and corrections may not be possible.

The Completion Time of 72 hours is allowed for restoring the TSP within limits, where possible, because 72 hours is the same time allowed for restoration of other ECCS components.

B.1 and B.2

If the TSP cannot be restored within limits within the Completion Time of Required Action A.1, the plant must be brought to a MODE in which the LCO does not apply. The specified Completion Times for reaching MODES 3 and 4 are those used throughout the Technical Specifications; they were chosen to allow reaching the specified conditions from full power in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.5.5.1

Periodic determination of the volume of TSP in containment must be performed due to the possibility of leaking valves and components in the containment building that could cause dissolution of the TSP during normal operation. A Frequency of 18 months is required to determine visually that a minimum of [291] cubic feet is contained in the TSP baskets. This requirement ensures that there is an adequate volume of TSP to adjust the pH of the post LOCA sump solution to a value ≥ 7.0.

The periodic verification is required every 18 months, since access to the TSP baskets is only feasible during outages, and normal fuel cycles are scheduled for 18 months. Operating experience has shown this Surveillance Frequency acceptable due to the margin in the volume of TSP placed in the containment building.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.5.5.2

Testing must be performed to ensure the solubility and buffering ability of the TSP after exposure to the containment environment. A representative sample of [ ] grams of TSP from one of the baskets in containment is submerged in 1.0 gal ± 0.05 gal of water at a boron concentration of [ ] ppm and at the standard temperature of 25°C ± 5°C. Without agitation, the solution pH should be raised to ≥ 7 within 4 hours. The representative sample weight is based on the minimum required TSP weight of [ ] kilograms, which at manufactured density corresponds to the minimum volume of [ ] cubic ft, and maximum possible post LOCA sump volume of [ ] gallons, normalized to buffer a 1.0 gal sample. The boron concentration of the test water is representative of the maximum possible boron concentration corresponding to the maximum possible post LOCA sump volume. Agitation of the test solution is prohibited, since an adequate standard for the agitation intensity cannot be specified. The test time of 4 hours is necessary to allow time for the dissolved TSP to naturally diffuse through the sample solution. In the post LOCA containment sump, rapid mixing would occur, significantly decreasing the actual amount of time before the required pH is achieved. This would ensure compliance with the Standard Review Plan requirement of a pH ≥ 7.0 by the onset of recirculation after a LOCA.

REFERENCES None.

B 3.6 CONTAINMENT SYSTEMS

B 3.6.1A Containment (Atmospheric)

BASES

BACKGROUND

The containment consists of the concrete reactor building (RB), its steel liner, and the penetrations through this structure. The structure is designed to contain radioactive material that may be released from the reactor core following a design basis loss of coolant accident (LOCA). Additionally, this structure provides shielding from the fission products that may be present in the containment atmosphere following accident conditions.

The containment is a reinforced concrete structure with a cylindrical wall, a flat foundation mat, and a shallow dome roof. For containments with ungrouted tendons, the cylinder wall is prestressed with a post tensioning system in the vertical and horizontal directions, and the dome roof is prestressed utilizing a three way post tensioning system. The inside surface of the containment is lined with a carbon steel liner to ensure a high degree of leak tightness during operating and accident conditions.

The concrete RB is required for structural integrity of the containment under Design Basis Accident (DBA) conditions. The steel liner and its penetrations establish the leakage limiting boundary of the containment. Maintaining the containment OPERABLE limits the leakage of fission product radioactivity from the containment to the environment. SR 3.6.1.1 leakage rate requirements comply with 10 CFR 50, Appendix J, Option [A][B] (Ref. 1), as modified by approved exemptions.

The isolation devices for the penetrations in the containment boundary are a part of the containment leak tight barrier. To maintain this leak tight barrier:

a. All penetrations required to be closed during accident conditions are either:

    1. Capable of being closed by an OPERABLE automatic containment isolation system or

    2. Closed by manual valves, blind flanges, or de-activated automatic valves secured in their closed positions, except as provided in LCO 3.6.3, "Containment Isolation Valves,"

BASES

BACKGROUND (continued)

b. Each air lock is OPERABLE, except as provided in LCO 3.6.2, "Containment Air Locks,"

c. All equipment hatches are closed, and

[d. The pressurized sealing mechanism associated with a penetration, except as provided in LCO 3.6.[ ], is OPERABLE.]

APPLICABLE SAFETY ANALYSES

The safety design basis for the containment is that the containment must withstand the pressures and temperatures of the limiting DBA without exceeding the design leakage rate.

The DBAs that result in a release of radioactive material within containment are a LOCA, a main steam line break, and a control element assembly ejection accident (Ref. 2). In the analysis of each of these accidents, it is assumed that containment is OPERABLE such that release of fission products to the environment is controlled by the rate of containment leakage. The containment was designed with an allowable leakage rate of [0.10]% of containment air weight per day (Ref. 3). This leakage rate is defined in 10 CFR 50, Appendix J, Option [A][B], (Ref. 1), as L_a: the maximum allowable containment leakage rate at the calculated maximum peak containment pressure (P_a) of [55.7] psig, which results from the limiting design basis LOCA (Ref. 2).

Satisfactory leakage rate test results are a requirement for the establishment of containment OPERABILITY.

The containment satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

Containment OPERABILITY is maintained by limiting leakage to $\leq 1.0\ L_a$, except prior to the first startup after performing a required Containment Leakage Rate Testing Program leakage test. At this time, the applicable leakage limits must be met.

Compliance with this LCO will ensure a containment configuration, including equipment hatches, that is structurally sound and that will limit leakage to those leakage rates assumed in the safety analysis.

Individual leakage rates specified for the containment air lock (LCO 3.6.2) [and purge valves with resilient seals (LCO 3.6.3)] are not specifically part of the acceptance criteria of 10 CFR 50, Appendix J. Therefore, leakage rates exceeding these individual limits only result in the containment being inoperable when the leakage results in exceeding the overall acceptance criteria of $1.0\ L_a$.

BASES

APPLICABILITY

In MODES 1, 2, 3, and 4, a DBA could cause a release of radioactive material into containment. In MODES 5 and 6, the probability and consequences of these events are reduced due to the pressure and temperature limitations of these MODES. Therefore, containment is not required to be OPERABLE in MODE 5 to prevent leakage of radioactive material from containment. The requirements for containment during MODE 6 are addressed in LCO 3.9.3, "Containment Penetrations."

ACTIONS

A.1

In the event containment is inoperable, containment must be restored to OPERABLE status within 1 hour. The 1 hour Completion Time provides a period of time to correct the problem commensurate with the importance of maintaining containment during MODES 1, 2, 3, and 4. This time period also ensures that the probability of an accident (requiring containment OPERABILITY) occurring during periods when containment is inoperable is minimal.

B.1 and B.2

If containment cannot be restored to OPERABLE status within the required Completion Time, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 5 within 36 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.6.1.1

Maintaining the containment OPERABLE requires compliance with the visual examinations and leakage rate test requirements of the Containment Leakage Rate Testing Program.

The containment concrete visual examinations may be performed during either power operation, e.g., performed concurrently with other containment inspection-related activities such as tendon testing, or during a maintenance or refueling outage. The visual examinations of the steel liner plate inside containment are performed during maintenance or refueling outages since this is the only time the liner plate is fully accessible.

BASES

SURVEILLANCE REQUIREMENTS (continued)

Failure to meet air lock and purge valve with resilient seal leakage limits specified in LCO 3.6.2 and LCO 3.6.3 does not invalidate the acceptability of these overall leakage determinations unless their contribution to overall Type A, B, and C leakage causes that to exceed limits. As left leakage prior to the first startup after performing a required Containment Leakage Rate Testing Program leakage test is required to be $< 0.6\ L_a$ for combined Type B and C leakage, and [$< 0.75\ L_a$ for Option A] [$\leq 0.75\ L_a$ for Option B] for overall Type A leakage. At all other times between required leakage rate tests, the acceptance criteria is based on an overall Type A leakage limit of $\leq 1.0\ L_a$. At $\leq 1.0\ L_a$ the offsite dose consequences are bounded by the assumptions of the safety analysis. SR Frequencies are as required by the Containment Leakage Rate Testing Program. These periodic testing requirements verify that the containment leakage rate does not exceed the leakage rate assumed in the safety analysis.

SR Frequencies are as required by the Containment Leakage Rate Testing Program. These periodic testing requirements verify that the containment leakage rate does not exceed the leakage rate assumed in the safety analysis.

----------------------------------REVIEWER'S NOTE----------------------------------
Regulatory Guide 1.163 and NEI 94-01 include acceptance criteria for as-left and as-found Type A leakage rates and combined Type B and C leakage rates, which may be reflected in the Bases.

[SR 3.6.1.2

For ungrouted, post tensioned tendons, this SR ensures that the structural integrity of the containment will be maintained in accordance with the provisions of the Containment Tendon Surveillance Program. Testing and Frequency are in accordance with the ASME Code, Section XI, Subsection IWL (Ref. 4), and applicable addenda as required by 10 CFR 50.55a.]

REFERENCES

1. 10 CFR 50, Appendix J, Option [A][B].
2. FSAR, Section [ ].
3. FSAR, Section [ ].
4. ASME Code, Section XI, Subsection IWL.

B 3.6 CONTAINMENT SYSTEMS

B 3.6.1B Containment (Dual)

BASES

BACKGROUND

The containment is a free standing steel pressure vessel surrounded by a reinforced concrete shield building. The containment vessel, including all its penetrations, is a low leakage steel shell designed to contain radioactive material that may be released from the reactor core following a design basis loss of coolant accident (LOCA). Additionally, the containment and shield building provide shielding from the fission products that may be present in the containment atmosphere following accident conditions.

The containment vessel is a vertical cylindrical steel pressure vessel with hemispherical dome and ellipsoidal bottom, completely enclosed by a reinforced concrete shield building. A 4 ft wide annular space exists between the walls and domes of the steel containment vessel and the concrete shield building to permit inservice inspection and collection of containment outleakage. Dual containments utilize an outer concrete building for shielding and an inner steel containment for leak tightness.

Containment piping penetration assemblies provide for the passage of process, service, sampling, and instrumentation pipelines into the containment vessel while maintaining containment OPERABILITY. The shield building provides biological shielding and allows controlled release of the annulus atmosphere under accident conditions, as well as environmental missile protection for the containment vessel and the Nuclear Steam Supply System.

The inner steel containment and its penetrations establish the leakage limiting boundary of the containment. Maintaining the containment OPERABLE limits the leakage of fission product radioactivity from the containment to the environment. Loss of containment OPERABILITY could cause site boundary doses, in the event of a Design Basis Accident (DBA), to exceed values given in the licensing basis. SR 3.6.1.1 leakage rate requirements comply with 10 CFR 50, Appendix J, Option [A][B] (Ref. 1), as modified by approved exemptions.

The isolation devices for the penetrations in the containment boundary are a part of the containment leak tight barrier. To maintain this leak tight barrier:

BASES

BACKGROUND (continued)

a. All penetrations required to be closed during accident conditions are either:

1. Capable of being closed by an OPERABLE automatic containment isolation system or

2. Closed by manual valves, blind flanges, or de-activated automatic valves secured in their closed positions, except as provided in LCO 3.6.3, "Containment Isolation Valves,"

b. Each air lock is OPERABLE except as provided in LCO 3.6.2, "Containment Air Locks,"

c. All equipment hatches are closed, and

[d. The pressurized sealing mechanism associated with a penetration, except as provided in LCO 3.6.[ ], is OPERABLE.]

APPLICABLE SAFETY ANALYSES

The safety design basis for the containment is that the containment must withstand the pressures and temperatures of the limiting DBA without exceeding the design leakage rate.

The DBAs that result in a release of radioactive material within containment are a LOCA, a main steam line break, and a control element assembly ejection accident (Ref. 2). In the analysis of each of these accidents, it is assumed that containment is OPERABLE such that release of fission products to the environment is controlled by the rate of containment leakage. The containment was designed with an allowable leakage rate of [0.50]% of containment air weight per day (Ref. 3). This leakage rate is defined in 10 CFR 50, Appendix J, Option [A][B] (Ref. 1), as L_a: the maximum allowable containment leakage rate at the calculated maximum peak containment pressure (P_a) of [42.3] psig, which results from the limiting design basis LOCA (Ref. 2).

Satisfactory leakage rate test results are a requirement for the establishment of containment OPERABILITY.

The containment satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO

Containment OPERABILITY is maintained by limiting leakage to ≤ 1.0 L_a, except prior to the first startup after performing a required Containment Leakage Rate Testing Program leakage test. At this time, the applicable leakage limits must be met.

Compliance with this LCO will ensure a containment configuration, including equipment hatches, that is structurally sound and that will limit leakage to those leakage rates assumed in the safety analysis.

Individual leakage rates specified for the containment air lock (LCO 3.6.2) [, purge valves with resilient seals, and secondary bypass leakage (LCO 3.6.3)] are not specifically part of the acceptance criteria of 10 CFR 50, Appendix J. Therefore, leakage rates exceeding these individual limits only result in the containment being inoperable when the leakage results in exceeding the overall acceptance criteria of 1.0 L_a.

APPLICABILITY

In MODES 1, 2, 3, and 4, a DBA could cause a release of radioactive material into containment. In MODES 5 and 6, the probability and consequences of these events are reduced due to the pressure and temperature limitations of these MODES. Therefore, containment is not required to be OPERABLE in MODE 5 to prevent leakage of radioactive material from containment. The requirements for containment during MODE 6 refueling operations are addressed in LCO 3.9.3, "Containment Penetrations."

ACTIONS

A.1

In the event that containment is inoperable, it must be restored to OPERABLE status within 1 hour. The 1 hour Completion Time provides a period of time to correct the problem commensurate with the importance of maintaining containment OPERABLE during MODES 1, 2, 3, and 4. This time period also ensures that the probability of an accident (requiring containment OPERABILITY) occurring during periods when containment is inoperable is minimal.

B.1 and B.2

If containment cannot be restored to OPERABLE status within the required Completion Time, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 5 within 36 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.6.1.1

Maintaining containment OPERABLE requires compliance with the visual examinations and leakage rate test requirements of the Containment Leakage Rate Testing Program. The containment concrete visual examinations may be performed during either power operation, e.g., performed concurrently with other containment inspection-related activities such as tendon testing, or during a maintenance or refueling outage. The visual examinations of the steel liner plate inside containment are performed during maintenance or refueling outages since this is the only time the liner plate is fully accessible.

Failure to meet air lock and purge valve with resilient seal specific leakage limits specified in LCO 3.6.2 and LCO 3.6.3 does not invalidate the acceptability of these overall leakage determinations unless their contribution to overall Type A, B, and C leakage causes that to exceed limits. As left leakage prior to the first startup after performing a required Containment Leakage Rate Testing Program leakage test is required to be $< 0.6\ L_a$ for combined Type B and C leakage, and [$< 0.75\ L_a$ for Option A] [$\leq 0.75\ L_a$ for Option B] for overall Type A leakage. At all other times between required leakage rate tests, the acceptance criteria is based on an overall Type A leakage limit of $\leq 1.0\ L_a$. At $\leq 1.0\ L_a$ the offsite dose consequences are bounded by the assumptions of the safety analysis. SR Frequencies are as required by the Containment Leakage Rate Testing Program. These periodic testing requirements verify that the containment leakage rate does not exceed the leakage rate assumed in the safety analysis.

SR Frequencies are as required by the Containment Leakage Rate Testing Program. These periodic testing requirements verify that the containment leakage rate does not exceed the leakage rate assumed in the safety analysis.

----------------------------------REVIEWER'S NOTE----------------------------------
Regulatory Guide 1.163 and NEI 94-01 include acceptance criteria for as-left and as-found Type A leakage rates and combined Type B and C leakage rates, which may be reflected in the Bases.

[SR 3.6.1.2

For ungrouted, post tensioned tendons, this SR ensures that the structural integrity of the containment will be maintained in accordance with the provisions of the Containment Tendon Surveillance Program. Testing and Frequency are in accordance with the ASME Code, Section XI, Subsection IWL (Ref. 4), and applicable addenda as required by 10 CFR 50.55a.]

BASES

REFERENCES	1.	10 CFR 50, Appendix J, Option [A][B].
	2.	FSAR, Section [ ].
	3.	FSAR, Section [ ].
	4.	ASME Code, Section XI, Subsection IWL.

B 3.6 CONTAINMENT SYSTEMS

B 3.6.2 Containment Air Locks (Atmospheric and Dual)

BASES

BACKGROUND

Containment air locks form part of the containment pressure boundary and provide a means for personnel access during all MODES of operation.

Each air lock is nominally a right circular cylinder, 10 ft in diameter, with a door at each end. The doors are interlocked to prevent simultaneous opening. During periods when containment is not required to be OPERABLE, the door interlock mechanism may be disabled, allowing both doors of an air lock to remain open for extended periods when frequent containment entry is necessary. Each air lock door has been designed and tested to certify its ability to withstand a pressure in excess of the maximum expected pressure following a Design Basis Accident (DBA) in containment. As such, closure of a single door supports containment OPERABILITY. Each of the doors contains double gasketed seals and local leakage rate testing capability to ensure pressure integrity. To effect a leak tight seal, the air lock design uses pressure seated doors (i.e., an increase in containment internal pressure results in increased sealing force on each door).

Each personnel air lock is provided with limit switches on both doors that provide control room indication of door position. Additionally, control room indication is provided to alert the operator whenever an air lock door interlock mechanism is defeated.

The containment air locks form part of the containment pressure boundary. As such, air lock integrity and leak tightness is essential for maintaining the containment leakage rate within limit in the event of a DBA. Not maintaining air lock integrity or leak tightness may result in a leakage rate in excess of that assumed in the unit safety analysis.

APPLICABLE SAFETY ANALYSES

[For atmospheric containment, the DBAs that result in a release of radioactive material within containment are a loss of coolant accident (LOCA), a main steam line break (MSLB) and a control element assembly (CEA) ejection accident (Ref. 2). In the analysis of each of these accidents, it is assumed that containment is OPERABLE such that release of fission products to the environment is controlled by the rate of containment leakage. The containment was designed with an allowable leakage rate of [0.10]% of containment air weight per day (Ref. 3). This leakage rate is defined in 10 CFR 50, Appendix J, Option A (Ref. 1), as

BASES

APPLICABLE SAFETY ANALYSES (continued)

L_a: the maximum allowable containment leakage rate at the calculated [maximum] peak containment pressure (P_a) of [55.7] psig, which results from the limiting design basis LOCA. This allowable leakage rate forms the basis for the acceptance criteria imposed on the SRs associated with the air lock.

For dual containment, the DBAs that result in a release of radioactive material within containment are a LOCA, an MSLB, and a CEA ejection accident (Ref. 2). In the analysis of each of these accidents, it is assumed that containment is OPERABLE such that release of fission products to the environment is controlled by the rate of containment leakage. The containment was designed with an allowable leakage rate of [0.50]% of containment air weight per day (Ref. 3). This leakage rate is defined in 10 CFR 50, Appendix J, Option A (Ref. 1), as L_a: the maximum allowable containment leakage rate at the calculated [maximum] peak containment pressure (P_a) of [42.3] psig, which results from the limiting design basis LOCA. This allowable leakage rate forms the basis for the acceptance criteria imposed on the SRs associated with the air lock.]

The containment air locks satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

Each containment air lock forms part of the containment pressure boundary. As part of the containment pressure boundary, the air lock safety function is related to control of the containment leakage rate resulting from a DBA. Thus, each air lock's structural integrity and leak tightness are essential to the successful mitigation of such an event.

Each air lock is required to be OPERABLE. For the air lock to be considered OPERABLE, the air lock interlock mechanism must be OPERABLE, the air lock must be in compliance with the Type B air lock leakage test, and both air lock doors must be OPERABLE. The interlock allows only one air lock door of an air lock to be opened at one time. This provision ensures that a gross breach of containment does not exist when containment is required to be OPERABLE. Closure of a single door in each air lock is sufficient to provide a leak tight barrier following postulated events. Nevertheless, both doors are kept closed when the air lock is not being used for normal entry into or exit from containment.

BASES

APPLICABILITY

In MODES 1, 2, 3, and 4, a DBA could cause a release of radioactive material to containment. In MODES 5 and 6, the probability and consequences of these events are reduced due to the pressure and temperature limitations of these MODES. Therefore, the containment air locks are not required in MODE 5 to prevent leakage of radioactive material from containment. The requirements for the containment air locks during MODE 6 are addressed in LCO 3.9.3, "Containment Penetrations."

ACTIONS

The ACTIONS are modified by a Note that allows entry and exit to perform repairs on the affected air lock component. If the outer door is inoperable, then it may be easily accessed for most repairs. It is preferred that the air lock be accessed from inside primary containment by entering through the other OPERABLE air lock. However, if this is not practicable, or if repairs on either door must be performed from the barrel side of the door then it is permissible to enter the air lock through the OPERABLE door, which means there is a short time during which the containment boundary is not intact (during access through the OPERABLE door). The ability to open the OPERABLE door, even if it means the containment boundary is temporarily not intact, is acceptable because of the low probability of an event that could pressurize the containment during the short time in which the OPERABLE door is expected to be open. After each entry and exit, the OPERABLE door must be immediately closed. If ALARA conditions permit, entry and exit should be via an OPERABLE air lock.

A second Note has been added to provide clarification that, for this LCO, separate Condition entry is allowed for each air lock. This is acceptable, since the Required Actions for each Condition provide appropriate compensatory actions for each inoperable air lock. Complying with the Required Actions may allow for continued operation, and a subsequent inoperable air lock is governed by subsequent Condition entry and application of associated Required Actions. A third Note has been included that requires entry into the applicable Conditions and Required Actions of LCO 3.6.1, "Containment," when leakage results in exceeding the overall containment leakage limit.

<u>A.1, A.2, and A.3</u>

With one air lock door inoperable in one or more containment air locks, the OPERABLE door must be verified closed (Required Action A.1) in each affected containment air lock. This ensures that a leak tight containment barrier is maintained by the use of an OPERABLE air lock door. This action must be completed within 1 hour. This specified time period is consistent with the ACTIONS of LCO 3.6.1, which requires containment be restored to OPERABLE status within 1 hour.

BASES

ACTIONS (continued)

In addition, the affected air lock penetration must be isolated by locking closed an OPERABLE air lock door within the 24 hour Completion Time. The 24 hour Completion Time is considered reasonable for locking the OPERABLE air lock door, considering the OPERABLE door of the affected air lock is being maintained closed.

Required Action A.3 verifies that an air lock with an inoperable door has been isolated by the use of a locked and closed OPERABLE air lock door. This ensures that an acceptable containment leakage boundary is maintained. The Completion Time of once per 31 days is based on engineering judgment and is considered adequate in view of the low likelihood of a locked door being mispositioned and other administrative controls. Required Action A.3 is modified by a Note that applies to air lock doors located in high radiation areas and allows these doors to be verified locked closed by use of administrative means. Allowing verification by administrative means is considered acceptable, since access to these areas is typically restricted. Therefore, the probability of misalignment of the door, once it has been verified to be in the proper position, is small.

The Required Actions have been modified by two Notes. Note 1 ensures that only the Required Actions and associated Completion Times of Condition C are required if both doors in the same air lock are inoperable. With both doors in the same air lock inoperable, an OPERABLE door is not available to be closed. Required Actions C.1 and C.2 are the appropriate remedial actions. The exception of Note 1 does not affect tracking the Completion Time from the initial entry into Condition A; only the requirement to comply with the Required Actions. Note 2 allows use of the air lock for entry and exit for 7 days under administrative controls if both air locks have an inoperable door. This 7 day restriction begins when the second air lock is discovered inoperable. Containment entry may be required to perform Technical Specifications (TS) Surveillances and Required Actions, as well as other activities on equipment inside containment that are required by TS or activities on equipment that support TS-required equipment. This Note is not intended to preclude performing other activities (i.e., non-TS-required activities) if the containment was entered, using the inoperable air lock, to perform an allowed activity listed above. This allowance is acceptable due to the low probability of an event that could pressurize the containment during the short time that the OPERABLE door is expected to be open.

BASES

ACTIONS (continued)

B.1, B.2, and B.3

With an air lock interlock mechanism inoperable in one or more air locks, the Required Actions and associated Completion Times are consistent with those specified in Condition A.

The Required Actions have been modified by two Notes. Note 1 ensures that only the Required Actions and associated Completion Times of Condition C are required if both doors in the same air lock are inoperable. With both doors in the same air lock inoperable, an OPERABLE door is not available to be closed. Required Actions C.1 and C.2 are the appropriate remedial actions. Note 2 allows entry into and exit from containment under the control of a dedicated individual stationed at the air lock to ensure that only one door is opened at a time (i.e., the individual performs the function of the interlock).

Required Action B.3 is modified by a Note that applies to air lock doors located in high radiation areas and allows these doors to be verified locked closed by use of administrative means. Allowing verification by administrative means is considered acceptable, since access to these areas is typically restricted. Therefore, the probability of misalignment of the door, once it has been verified to be in the proper position, is small.

C.1, C.2, and C.3

With one or more air locks inoperable for reasons other than those described in Condition A or B, Required Action C.1 requires action to be initiated immediately to evaluate previous combined leakage rates using current air lock test results. An evaluation is acceptable since it is overly conservative to immediately declare the containment inoperable if both doors in an air lock have failed a seal test or if the overall air lock leakage is not within limits. In many instances (e.g., only one seal per door has failed), containment remains OPERABLE, yet only 1 hour (per LCO 3.6.1) would be provided to restore the air lock door to OPERABLE status prior to requiring a plant shutdown. In addition, even with both doors failing the seal test, the overall containment leakage rate can still be within limits.

Required Action C.2 requires that one door in the affected containment air lock must be verified to be closed. This action must be completed within the 1 hour Completion Time. This specified time period is consistent with the ACTIONS of LCO 3.6.1, which requires that containment be restored to OPERABLE status within 1 hour.

BASES

ACTIONS (continued)

Additionally, the affected air lock(s) must be restored to OPERABLE status within the 24 hour Completion Time. The specified time period is considered reasonable for restoring an inoperable air lock to OPERABLE status, assuming that at least one door is maintained closed in each affected air lock.

D.1 and D.2

If the inoperable containment air lock cannot be restored to OPERABLE status within the required Completion Time, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 5 within 36 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.6.2.1

Maintaining containment air locks OPERABLE requires compliance with the leakage rate test requirements of the Containment Leakage Rate Testing Program. This SR reflects the leakage rate testing requirements with regard to air lock leakage (Type B leakage tests). The acceptance criteria were established during initial air lock and containment OPERABILITY testing. The periodic testing requirements verify that the air lock leakage does not exceed the allowed fraction of the overall containment leakage rate. The Frequency is required by the Containment Leakage Rate Testing Program.

The SR has been modified by two Notes. Note 1 states that an inoperable air lock door does not invalidate the previous successful performance of the overall air lock leakage test. This is considered reasonable since either air lock door is capable of providing a fission product barrier in the event of a DBA. Note 2 has been added to this SR requiring the results to be evaluated against the acceptance criteria which is applicable to SR 3.6.1.1. This ensures that air lock leakage is properly accounted for in determining the combined Type B and C containment leakage rate.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.6.2.2

The air lock interlock is designed to prevent simultaneous opening of both doors in a single air lock. Since both the inner and outer doors of an air lock are designed to withstand the maximum expected post accident containment pressure, closure of either door will support containment OPERABILITY. Thus, the door interlock feature supports containment OPERABILITY while the air lock is being used for personnel transit into and out of containment. Periodic testing of this interlock demonstrates that the interlock will function as designed and that simultaneous opening of the inner and outer doors will not inadvertently occur. Due to the purely mechanical nature of this interlock, and given that the interlock mechanism is not normally challenged when the containment airlock door is used for entry and exit (procedures require strict adherence to single door opening), this test is only required to be performed every 24 months. The 24 month Frequency is based on the need to perform this Surveillance under the conditions that apply during a plant outage, and the potential for loss of containment OPERABILITY if the Surveillance were performed with the reactor at power. The 24 month Frequency for the interlock is justified based on generic operating experience. The 24 month Frequency is based on engineering judgment and is considered adequate given that the interlock is not challenged during the use of the airlock.

REFERENCES

1. 10 CFR 50, Appendix J, Option [A][B].
2. FSAR, Section [ ].
3. FSAR, Section [ ].

B 3.6 CONTAINMENT SYSTEMS

B 3.6.3 Containment Isolation Valves (Atmospheric and Dual)

BASES

BACKGROUND

The containment isolation valves form part of the containment pressure boundary and provide a means for fluid penetrations not serving accident consequence limiting systems to be provided with two isolation barriers that are closed on an automatic isolation signal. These isolation devices are either passive or active (automatic). Manual valves, de-activated automatic valves secured in their closed position (including check valves with flow through the valve secured), blind flanges, and closed systems are considered passive devices. Check valves, or other automatic valves designed to close without operator action following an accident, are considered active devices. Two barriers in series are provided for each penetration so that no single credible failure or malfunction of an active component can result in a loss of isolation or leakage that exceeds limits assumed in the safety analysis. One of these barriers may be a closed system.

Containment isolation occurs upon receipt of a high containment pressure signal or a low Reactor Coolant System (RCS) pressure signal. The containment isolation signal closes automatic containment isolation valves in fluid penetrations not required for operation of Engineered Safety Feature systems in order to prevent leakage of radioactive material. Upon actuation of safety injection, automatic containment isolation valves also isolate systems not required for containment or RCS heat removal. Other penetrations are isolated by the use of valves in the closed position or blind flanges. As a result, the containment isolation valves (and blind flanges) help ensure that the containment atmosphere will be isolated in the event of a release of radioactive material to containment atmosphere from the RCS following a Design Basis Accident (DBA).

The OPERABILITY requirements for containment isolation valves help ensure that containment is isolated within the time limits assumed in the safety analysis. Therefore, the OPERABILITY requirements provide assurance that the containment function assumed in the accident analysis will be maintained.

The purge valves were designed for intermittent operation, providing a means of removing airborne radioactivity caused by minor RCS leakage prior to personnel entry into containment. There are two sets of purge valves: normal purge and exhaust valves and minipurge and exhaust valves. The normal and minipurge supply and exhaust lines are each supplied with inside and outside containment isolation valves but share common supply and exhaust penetration lines.

BASES

BACKGROUND (continued)

The normal purge valves are designed for purging the containment atmosphere to the unit stack while introducing filtered makeup from the outside to provide adequate ventilation for personnel comfort when the unit is shut down during refueling operations and maintenance. Motor operated isolation valves are provided inside the containment, and air operated isolation valves are provided outside the containment. The valves are operated manually from the control room. The valves will close automatically upon receipt of a containment purge isolation signal. The air operated valves fail closed upon a loss of air. Because of their large size, the normal purge valves in some units are not qualified for automatic closure from their open position under DBA conditions. Therefore, the normal purge valves are normally maintained closed in MODES 1, 2, 3, and 4 to ensure the containment boundary is maintained.

Open normal purge valves, or a failure of the minipurge valves to close, following an accident that releases contamination to the containment atmosphere would cause a significant increase in the containment leakage rate.

APPLICABLE SAFETY ANALYSES

The containment isolation valve LCO was derived from the assumptions related to minimizing the loss of reactor coolant inventory and establishing the containment boundary during major accidents. As part of the containment boundary, containment isolation valve OPERABILITY supports leak tightness of the containment. Therefore, the safety analysis of any event requiring isolation of containment is applicable to this LCO.

The DBAs that result in a release of radioactive material within containment are a loss of coolant accident (LOCA), a main steam line break, and a control element assembly ejection accident. In the analysis for each of these accidents, it is assumed that containment isolation valves are either closed or function to close within the required isolation time following event initiation. This ensures that potential paths to the environment through containment isolation valves (including containment purge valves) are minimized. The safety analysis assumes that the normal purge valves are closed at event initiation.

The DBA analysis assumes that, within 60 seconds after the accident, isolation of the containment is complete and leakage terminated except for the design leakage rate, L_a. The containment isolation total response time of 60 seconds includes signal delay, diesel generator startup (for loss of offsite power), and containment isolation valve stroke times.

BASES

APPLICABLE SAFETY ANALYSES (continued)

The single failure criterion required to be imposed in the conduct of unit safety analyses was considered in the original design of the containment purge valves. Two valves in series on each purge line provide assurance that both the supply and exhaust lines could be isolated even if a single failure occurred. The inboard and outboard isolation valves on each line are provided with diverse power sources, motor operated and pneumatically operated spring closed, respectively. This arrangement was designed to preclude common mode failures from disabling both valves on a purge line.

The purge valves may be unable to close in the environment following a LOCA. Therefore, each of the purge valves is required to remain sealed closed during MODES 1, 2, 3, and 4. In this case, the single failure criterion remains applicable to the containment purge valves due to failure in the control circuit associated with each valve. Again, the purge system valve design precludes a single failure from compromising the containment boundary as long as the system is operated in accordance with the subject LCO. The minipurge valves are capable of closing under accident conditions. Therefore, they are allowed to be open for limited periods during power operation.

The containment isolation valves satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

Containment isolation valves form a part of the containment boundary. The containment isolation valve safety function is related to minimizing the loss of reactor coolant inventory and establishing the containment boundary during a DBA.

The automatic power operated isolation valves are required to have isolation times within limits and to actuate on an automatic isolation signal. The purge valves must be maintained sealed closed [or have blocks installed to prevent full opening]. [Blocked purge valves also actuate on an automatic signal.] The valves covered by this LCO are listed with their associated stroke times in the FSAR (Ref. 1).

The normally closed isolation valves are considered OPERABLE when manual valves are closed, automatic valves are de-activated and secured in their closed position, blind flanges are in place, and closed systems are intact. These passive isolation valves or devices are those listed in Reference 2.

BASES

LCO (continued)

Purge valves with resilient seals [and secondary containment bypass valves] must meet additional leakage rate requirements. The other containment isolation valve leakage rates are addressed by LCO 3.6.1, "Containment," as Type C testing.

This LCO provides assurance that the containment isolation valves and purge valves will perform their designed safety functions to minimize the loss of reactor coolant inventory and establish the containment boundary during accidents.

APPLICABILITY

In MODES 1, 2, 3, and 4, a DBA could cause a release of radioactive material to containment. In MODES 5 and 6, the probability and consequences of these events are reduced due to the pressure and temperature limitations of these MODES. Therefore, the containment isolation valves are not required to be OPERABLE in MODE 5. The requirements for containment isolation valves during MODE 6 are addressed in LCO 3.9.3, "Containment Penetrations."

ACTIONS

The ACTIONS are modified by a Note allowing penetration flow paths, except for [42] inch purge valve penetration flow paths, to be unisolated intermittently under administrative controls. These administrative controls consist of stationing a dedicated operator at the valve controls, who is in continuous communication with the control room. In this way, the penetration can be rapidly isolated when a need for containment isolation is indicated. Due to the size of the containment purge line penetration and the fact that those penetrations exhaust directly from the containment atmosphere to the environment, these valves may not be opened under administrative controls.

A second Note has been added to provide clarification that, for this LCO, separate Condition entry is allowed for each penetration flow path. This is acceptable, since the Required Actions for each Condition provide appropriate compensatory actions for each inoperable containment isolation valve. Complying with the Required Actions may allow for continued operation, and subsequent inoperable containment isolation valves are governed by subsequent Condition entry and application of associated Required Actions.

The ACTIONS are further modified by a third Note, which ensures that appropriate remedial actions are taken, if necessary, if the affected systems are rendered inoperable by an inoperable containment isolation valve.

BASES

ACTIONS (continued)

A fourth Note has been added that requires entry into the applicable Conditions and Required Actions of LCO 3.6.1 when leakage results in exceeding the overall containment leakage limit.

A.1 and A.2

In the event one containment isolation valve in one or more penetration flow paths is inoperable, the affected penetration flow path must be isolated. The method of isolation must include the use of at least one isolation barrier that cannot be adversely affected by a single active failure. Isolation barriers that meet this criterion are a closed and de-activated automatic containment isolation valve, a closed manual valve, a blind flange, and a check valve with flow through the valve secured. For penetrations isolated in accordance with Required Action A.1, the device used to isolate the penetration should be the closest available one to containment. Required Action A.1 must be completed within the 4 hour Completion Time. The 4 hour Completion Time is reasonable, considering the time required to isolate the penetration and the relative importance of supporting containment OPERABILITY during MODES 1, 2, 3, and 4 (Refs. 4 and 5).

For affected penetration flow paths that cannot be restored to OPERABLE status within the 4 hour Completion Time and that have been isolated in accordance with Required Action A.1, the affected penetration flow paths must be verified to be isolated on a periodic basis. This is necessary to ensure that containment penetrations required to be isolated following an accident and no longer capable of being automatically isolated will be in the isolation position should an event occur. This Required Action does not require any testing or device manipulation. Rather, it involves verification, through a system walkdown, that those isolation devices outside containment and capable of being mispositioned are in the correct position. The Completion Time of "once per 31 days for isolation devices outside containment" is appropriate considering the fact that the devices are operated under administrative controls and the probability of their misalignment is low. For the isolation devices inside containment, the time period specified as "prior to entering MODE 4 from MODE 5 if not performed within the previous 92 days" is based on engineering judgment and is considered reasonable in view of the inaccessibility of the isolation devices and other administrative controls that will ensure that isolation device misalignment is an unlikely possibility.

BASES

ACTIONS (continued)

Condition A has been modified by a Note indicating that this Condition is only applicable to [the containment sump supply valves to the ECCS and containment spray pumps].

----------------------------------REVIEWER'S NOTE----------------------------------
Condition A is only applicable to the containment isolation valves that do not meet the conditions to extend the Completion Time to 7 days.

Required Action A.2 is modified by two Notes. Note 1 applies to isolation devices located in high radiation areas and allows these devices to be verified closed by use of administrative means. Allowing verification by administrative means is considered acceptable, since access to these areas is typically restricted. Note 2 applies to isolation devices that are locked, sealed, or otherwise secured in position and allows these devices to be verified closed by use of administrative means. Allowing verification by administrative means is considered acceptable, since the function of locking, sealing, or securing components is to ensure that these devices are not inadvertently repositioned. Therefore, the probability of misalignment of these devices, once they have been verified to be in the proper position, is small.

B.1 and B.2

----------------------------------REVIEWER'S NOTE----------------------------------
Adoption of the 7 day Completion Time is contingent on the conditions identified in Reference 4.

1. Individual licensees requesting CIV Completion Time relaxations should state in their plant-specific application that they have verified that the Joint Applications Report (JAR) results apply to their plant. Licensees should verify that the relaxed Completion Times will only apply to penetrations analyzed to meet the risk guidelines of Regulatory Guide 1.177 and fall within the 14 containment penetration configurations considered in the JAR. Any other containment penetration configurations not analyzed in the JAR must be supported by a plant-specific analysis. Licensee submittals must retain the current Completion Times for the three configurations that were not analyzed in the JAR: containment sump supply valves to the ECCS and containment spray systems pumps, valves associated with the main feedwater system, and main steam isolation valves.

BASES

ACTIONS (continued)

2. Licensees should provide sufficient quantitative or qualitative substantiation to demonstrate that external events will not affect the results of the analysis supporting the extended Completion Times.

3. Licensees should state that they have verified acceptable PRA quality as described in Regulatory Guide 1.177.

4. Licensees should require verification of the operability of the remaining CIV(s) in a penetration flow path before entering the extended Completion Time for corrective maintenance. The JAR assumes that the penetrations remain physically intact in MODES in which these valves are to be operable during corrective maintenance. Licensees should describe in their plant specific application how the affected penetration will remain physically intact, or state that the penetration will be isolated so as to not permit a release to the outside environment.

5. The licensee should consider the additive nature of multiple failed CIVs, and the possibility of entering multiple AOTs and verify that these situations will result in risks consistent with the incremental conditional core damage probability (ICCDP) and incremental large early release probability (ICLERP) guidelines so that defense-in-depth for the safety systems will be maintained.

[<u>B.1 and B.2</u>

In the event one containment isolation valve in one or more penetration flow paths is inoperable, [except for Condition A and for purge valve leakage and shield building bypass leakage not within limit], the affected penetration flow path must be isolated. The method of isolation must include the use of at least one isolation barrier that cannot be adversely affected by a single active failure. Isolation barriers that meet this criterion are a closed and de-activated automatic containment isolation valve, a closed manual valve, a blind flange, and a check valve with flow through the valve secured. For penetrations isolated in accordance with Required Action B.1, the device used to isolate the penetration should be the closest available one to containment. Required Action B.1 must be completed within the [7 day] Completion Time. The [7 day] Completion Time is reasonable, considering the time required to isolate the penetration and the relative importance of supporting containment OPERABILITY during MODES 1, 2, 3, and 4 (References 3 and 4).

BASES

ACTIONS (continued)

For affected penetration flow paths that cannot be restored to OPERABLE status within the [7 day] Completion Time and that have been isolated in accordance with Required Action B.1, the affected penetration flow paths must be verified to be isolated on a periodic basis. This is necessary to ensure that containment penetrations required to be isolated following an accident and no longer capable of being automatically isolated will be in the isolation position should an event occur. This Required Action does not require any testing or device manipulation. Rather, it involves verification that those isolation devices outside containment and capable of being mispositioned are in the correct position. The Completion Time of "once per 31 days for isolation devices outside containment" is appropriate considering the fact that the devices are operated under administrative controls and the probability of their misalignment is low. For the isolation devices inside containment, the time period specified as "prior to entering MODE 4 from MODE 5 if not performed within the previous 92 days" is based on engineering judgment and is considered reasonable in view of the inaccessibility of the isolation devices and other administrative controls that will ensure that isolation device misalignment is an unlikely possibility.

Condition B has been modified by a Note indicating that this Condition is only applicable to those penetration flow paths with two [or more] containment isolation valves. For penetration flow paths with only one containment isolation valve and a closed system, Condition D provides appropriate actions.

Required Action B.2 is modified by two Notes. Note 1 applies to isolation devices located in high radiation areas and allows these devices to be verified closed by use of administrative means. Allowing verification by administrative means is considered acceptable, since access to these areas is typically restricted. Note 2 applies to isolation devices that are locked, sealed, or otherwise secured in position and allows these devices to be verified closed by use of administrative means. Allowing verification by administrative means is considered acceptable, since the function of locking, sealing, or securing components is to ensure that these devices are not inadvertently repositioned. Therefore, the probability of misalignment of these devices, once they have been verified to be in the proper position, is small.]

BASES

ACTIONS (continued)

C.1

With two [or more] containment isolation valves in one or more penetration flow paths inoperable, [except for purge valve leakage and shield building bypass leakage not within limit], the affected penetration flow path must be isolated within 1 hour. The method of isolation must include the use of at least one isolation barrier that cannot be adversely affected by a single active failure. Isolation barriers that meet this criterion are a closed and de-activated automatic valve, a closed manual valve, and a blind flange. The 1 hour Completion Time is consistent with the ACTIONS of LCO 3.6.1. In the event the affected penetration is isolated in accordance with Required Action C.1, the affected penetration must be verified to be isolated on a periodic basis per Required Action B.2, which remains in effect. This periodic verification is necessary to assure leak tightness of containment and that penetrations requiring isolation following an accident are isolated. The Completion Time of once per 31 days for verifying each affected penetration flow path is isolated is appropriate considering the fact that the valves are operated under administrative controls and the probability of their misalignment is low.

Condition C is modified by a Note indicating this Condition is only applicable to penetration flow paths with two [or more] containment isolation valves. Condition B of this LCO addresses the condition of one containment isolation valve inoperable in this type of penetration flow path.

D.1 and D.2

With one or more penetration flow paths with one containment isolation valve inoperable, the inoperable valve must be restored to OPERABLE status or the affected penetration flow path must be isolated. The method of isolation must include the use of at least one isolation barrier that cannot be adversely affected by a single active failure. Isolation barriers that meet this criterion are a closed and de-activated automatic valve, a closed manual valve, and a blind flange. A check valve may not be used to isolate the affected penetration. Required Action D.1 must be completed within the [72] hour Completion Time for those penetrations that do not meet the 7 day Completion Time criteria and [7 days] for penetrations that do meet the 7 day Completion Time criteria. The specified time period is reasonable, considering the relative stability of the closed system (hence, reliability) to act as a penetration isolation boundary and the relative importance of supporting containment OPERABILITY during MODES 1, 2, 3, and 4. In the event the affected

BASES

ACTIONS (continued)

penetration is isolated in accordance with Required Action D.1, the affected penetration flow path must be verified to be isolated on a periodic basis. This is necessary to assure leak tightness of containment and that containment penetrations requiring isolation following an accident are isolated. The Completion Time of once per 31 days for verifying that each affected penetration flow path is isolated is appropriate considering the valves are operated under administrative controls and the probability of their misalignment is low.

Condition D is modified by a Note indicating that this Condition is only applicable to those penetration flow paths with only one containment isolation valve and a closed system. The closed system must meet the requirements of Reference 4. This Note is necessary since this Condition is written to specifically address those penetration flow paths in a closed system.

Required Action D.2 is modified by two Notes. Note 1 applies to valves and blind flanges located in high radiation areas and allows these devices to be verified closed by use of administrative means. Allowing verification by administrative means is considered acceptable, since access to these areas is typically restricted. Note 2 applies to isolation devices that are locked, sealed, or otherwise secured in position and allows these devices to be verified closed by use of administrative means. Allowing verification by administrative means is considered acceptable, since the function of locking, sealing, or securing components is to ensure that these devices are not inadvertently repositioned. Therefore, the probability of misalignment of these valves, once they have been verified to be in the proper position, is small.

[E.1

With the secondary containment bypass leakage rate (SR 3.6.3.9) [or purge valve leakage rate (SR 3.6.3.6)] not within limit, the assumptions of the safety analysis are not met. Therefore, the leakage must be restored to within limit. Restoration can be accomplished by isolating the penetration(s) that caused the limit to be exceeded by use of one closed and de-activated automatic valve, closed manual valve, or blind flange. When a penetration is isolated, the leakage rate for the isolated penetration is assumed to be the actual pathway leakage through the isolation device. If two isolation devices are used to isolate the penetration, the leakage rate is assumed to be the lesser actual pathway leakage of the two devices. The 4 hour Completion Time for secondary

BASES

ACTIONS (continued)

containment bypass leakage is reasonable considering the time required to restore the leakage by isolating the penetration(s) and the relative importance of secondary containment bypass leakage to the overall containment function. [The 24 hour Completion Time for purge valve leakage is acceptable considering the purge valves remain closed so that a gross breach of containment does not exist.]

----------------------------------REVIEWER'S NOTE-----------------------------------

[The bracketed options provided in ACTION E reflect options in plant design and options in adopting the associated leakage rate Surveillances.

The options (in both ACTION E and ACTION F for purge valve leakage, are based primarily on the design - if leakage rates can be measured separately for each purge valve, ACTION F is intended to apply. This would be required to be able to implement Required Action F.3. Should the design allow only for leak testing both purge valves simultaneously, then the Completion Time for ACTION E should include the "24 hours for purge valve leakage" and ACTION F should be eliminated.]]

[<u>F.1, F.2, and F.3</u>

In the event one or more containment purge valves in one or more penetration flow paths are not within the purge valve leakage limits, purge valve leakage must be restored to within limits, or the affected penetration must be isolated. The method of isolation must be by the use of at least one isolation barrier that cannot be adversely affected by a single active failure. Isolation barriers that meet this criterion are a [closed and de-activated automatic valve with resilient seals, a closed manual valve with resilient seals, or a blind flange]. A purge valve with resilient seals utilized to satisfy Required Action F.1 must have been demonstrated to meet the leakage requirements of SR 3.6.3.6. The specified Completion Time is reasonable, considering that one containment purge valve remains closed so that a gross breach of containment does not exist.

In accordance with Required Action F.2, this penetration flow path must be verified to be isolated on a periodic basis. The periodic verification is necessary to ensure that containment penetrations required to be isolated following an accident, which are no longer capable of being automatically isolated, will be in the isolation position should an event occur. This Required Action does not require any testing or valve manipulation. Rather, it involves verification that those isolation devices outside

BASES

ACTIONS (continued)

containment capable of being mispositioned are in the correct position. For the isolation devices inside containment, the time period specified as "prior to entering MODE 4 from MODE 5 if not performed within the previous 92 days" is based on engineering judgment and is considered reasonable in view of the inaccessibility of the isolation devices and other administrative controls that will ensure that isolation device misalignment is an unlikely possibility.

For the containment purge valve with resilient seal that is isolated in accordance with Required Action F.1, SR 3.6.3.6 must be performed at least once every [92] days. This assures that degradation of the resilient seal is detected and confirms that the leakage rate of the containment purge valve does not increase during the time the penetration is isolated. The normal Frequency for SR 3.6.3.6, 184 days, is based on an NRC initiative, Generic Issue B-20 (Ref. 6). Since more reliance is placed on a single valve while in this Condition, it is prudent to perform the SR more often. Therefore, a Frequency of once per [92] days was chosen and has been shown to be acceptable based on operating experience.

Required Action F.2 is modified by two Notes. Note 1 applies to isolation devices located in high radiation areas and allows these devices to be verified closed by use of administrative means. Allowing verification by administrative means is considered acceptable, since access to these areas is typically restricted. Note 2 applies to isolation devices that are locked, sealed, or otherwise secured in position and allows these devices to be verified closed by use of administrative means. Allowing verification by administrative means is considered acceptable, since the function of locking, sealing, or securing components is to ensure that these devices are not inadvertently repositioned.]

<u>G.1 and G.2</u>

If the Required Actions and associated Completion Times are not met, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 5 within 36 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

BASES

SURVEILLANCE REQUIREMENTS

[SR 3.6.3.1

Each [42] inch containment purge valve is required to be verified sealed closed at 31 day intervals. This Surveillance is designed to ensure that a gross breach of containment is not caused by an inadvertent or spurious opening of a containment purge valve. Detailed analysis of the purge valves failed to conclusively demonstrate their ability to close during a LOCA in time to limit offsite doses. Therefore, these valves are required to be in the sealed closed position during MODES 1, 2, 3, and 4. A containment purge valve that is sealed closed must have motive power to the valve operator removed. This can be accomplished by de-energizing the source of electric power or by removing the air supply to the valve operator. In this application, the term "sealed" has no connotation of leak tightness. The Frequency is a result of an NRC initiative, Generic Issue B-24 (Ref. 7), related to containment purge valve use during unit operations. This SR is not required to be met while in Condition E of this LCO. This is reasonable since the penetration flow path would be isolated.]

SR 3.6.3.2

This SR ensures that the minipurge valves are closed as required or, if open, open for an allowable reason. If a purge valve is open in violation of this SR, the valve is considered inoperable. If the inoperable valve is not otherwise known to have excessive leakage when closed, it is not considered to have leakage outside of limits. The SR is not required to be met when the purge valves are open for pressure control, ALARA or air quality considerations for personnel entry, or for Surveillances that require the valves to be open. The minipurge valves are capable of closing in the environment following a LOCA. Therefore, these valves are allowed to be open for limited periods of time. The 31 day Frequency is consistent with other containment isolation valve requirements discussed in SR 3.6.3.3.

SR 3.6.3.3

This SR requires verification that each containment isolation manual valve and blind flange located outside containment and not locked, sealed, or otherwise secured and required to be closed during accident conditions is closed. The SR helps to ensure that post accident leakage of radioactive fluids or gases outside the containment boundary is within design limits. This SR does not require any testing or valve manipulation. Rather, it involves verification that those containment isolation valves outside containment and capable of being mispositioned are in the correct

BASES

SURVEILLANCE REQUIREMENTS (continued)

position. Since verification of valve position for containment isolation valves outside containment is relatively easy, the 31 day Frequency is based on engineering judgment and was chosen to provide added assurance of the correct positions. Containment isolation valves that are open under administrative controls are not required to meet the SR during the time the valves are open. This SR does not apply to valves that are locked, sealed, or otherwise secured in the closed position, since these were verified to be in the correct position upon locking, sealing, or securing.

The Note applies to valves and blind flanges located in high radiation areas and allows these devices to be verified closed by use of administrative means. Allowing verification by administrative means is considered acceptable, since access to these areas is typically restricted during MODES 1, 2, 3, 4 and for ALARA reasons. Therefore, the probability of misalignment of these containment isolation valves, once they have been verified to be in the proper position, is small.

SR 3.6.3.4

This SR requires verification that each containment isolation manual valve and blind flange located inside containment and not locked, sealed, or otherwise secured and required to be closed during accident conditions is closed. The SR helps to ensure that post accident leakage of radioactive fluids or gases outside the containment boundary is within design limits. For containment isolation valves inside containment, the Frequency of "prior to entering MODE 4 from MODE 5 if not performed within the previous 92 days" is appropriate, since these containment isolation valves are operated under administrative controls and the probability of their misalignment is low. Containment isolation valves that are open under administrative controls are not required to meet the SR during the time that they are open. This SR does not apply to valves that are locked, sealed, or otherwise secured in the closed position, since these were verified to be in the correct position upon locking, sealing, or securing.

The Note allows valves and blind flanges located in high radiation areas to be verified closed by use of administrative means. Allowing verification by administrative means is considered acceptable, since access to these areas is typically restricted during MODES 1, 2, and 3 for ALARA reasons. Therefore, the probability of misalignment of these containment isolation valves, once they have been verified to be in their proper position, is small.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.6.3.5

Verifying that the isolation time of each automatic power operated containment isolation valve is within limits is required to demonstrate OPERABILITY. The isolation time test ensures the valve will isolate in a time period less than or equal to that assumed in the safety analysis. [The isolation time and Frequency of this SR are in accordance with the Inservice Testing Program or 92 days.]

SR 3.6.3.6

For containment purge valves with resilient seals, additional leakage rate testing beyond the test requirements of 10 CFR 50, Appendix J, Option [A][B], (Ref. 8), is required to ensure OPERABILITY. Operating experience has demonstrated that this type of seal has the potential to degrade in a shorter time period than do other seal types. Based on this observation and the importance of maintaining this penetration leak tight (due to the direct path between containment and the environment), a Frequency of 184 days was established as part of the NRC resolution of Generic Issue B-20, "Containment Leakage Due to Seal Deterioration" (Ref. 6).

Additionally, this SR must be performed within 92 days after opening the valve. The 92 day Frequency was chosen recognizing that cycling the valve could introduce additional seal degradation (beyond that occurring to a valve that has not been opened). Thus, decreasing the interval (from 184 days) is a prudent measure after a valve has been opened.

SR 3.6.3.7

Automatic containment isolation valves close on a containment isolation signal to prevent leakage of radioactive material from containment following a DBA. This SR ensures each automatic containment isolation valve will actuate to its isolation position on a containment isolation actuation signal. This Surveillance is not required for valves that are locked, sealed, or otherwise secured in the required position under administrative controls. The [18] month Frequency was developed considering it is prudent that this SR be performed only during a unit outage, since isolation of penetrations would eliminate cooling water flow and disrupt normal operation of many critical components. Operating experience has shown that these components usually pass this SR when performed on the [18] month Frequency. Therefore, the Frequency was concluded to be acceptable from a reliability standpoint.

BASES

SURVEILLANCE REQUIREMENTS (continued)

[SR 3.6.3.8

-----------------------------------REVIEWER'S NOTE-----------------------------------
This SR is only required for those units with resilient seal purge valves allowed to be open during [MODE 1, 2, 3, or 4] and having blocking devices on the valves that are not permanently installed.

Verifying that each [42] inch containment purge valve is blocked to restrict opening to ≤ [50]% is required to ensure that the valves can close under DBA conditions within the times assumed in the analyses of References 1 and 2. If a LOCA occurs, the purge valves must close to maintain containment leakage within the values assumed in the accident analysis. At other times when purge valves are required to be capable of closing (e.g., during movement of [recently] irradiated fuel assemblies), pressurization concerns are not present, thus the purge valves can be fully open. The [18] month Frequency is appropriate because the blocking devices are typically removed only during a refueling outage.]

[SR 3.6.3.9

This SR ensures that the combined leakage rate of all secondary containment bypass leakage paths is less than or equal to the specified leakage rate. This provides assurance that the assumptions in the safety analysis are met. The leakage rate of each bypass leakage path is assumed to be the maximum pathway leakage (leakage through the worse of the two isolation valves) unless the penetration is isolated by use of one closed and de-activated automatic valve, closed manual valve, or blind flange. In this case, the leakage rate of the isolated bypass leakage path is assumed to be the actual pathway leakage through the isolation device. If both isolation valves in the penetration are closed, the actual leakage rate is the lesser leakage rate of the two valves. The Frequency is required by the Containment Leakage Rate Testing Program. This SR simply imposes additional acceptance criteria.

[Bypass leakage is considered part of L_a. unless specifically exempted.]]

BASES

REFERENCES

1. FSAR, Section [ ].

2. FSAR, Section [ ].

3. Combustion Engineering Owners Group (CEOG) Joint Applications Report (JAR) CE-NPSD-1168, Joint Applications Report for Containment Isolation Valve AOT Extension, dated June 1999.

4. NRC Safety Evaluation for CEOG Joint Applications Report CE-NPSD-1168, "JAR for CIV AOT Extension," dated June 26, 2000.

5. Standard Review Plan 6.2.4.

6. Generic Issue B-20.

7. Generic Issue B-24.

8. 10 CFR 50, Appendix J, Option [A][B].

B 3.6 CONTAINMENT SYSTEMS

B 3.6.4A Containment Pressure (Atmospheric)

BASES

BACKGROUND

The containment pressure is limited during normal operation to preserve the initial conditions assumed in the accident analyses for a loss of coolant accident (LOCA) or main steam line break (MSLB). These limits also prevent the containment pressure from exceeding the containment design negative pressure differential with respect to the outside atmosphere in the event of inadvertent actuation of the Containment Spray System.

Containment pressure is a process variable that is monitored and controlled. The containment pressure limits are derived from the input conditions used in the containment functional analyses and the containment structure external pressure analysis. Should operation occur outside these limits coincident with a Design Basis Accident (DBA), post accident containment pressures could exceed calculated values.

APPLICABLE SAFETY ANALYSES

Containment internal pressure is an initial condition used in the DBA analyses to establish the maximum peak containment internal pressure. The limiting DBAs considered for determining the maximum containment internal pressure (P_a) are the LOCA and MSLB. An MSLB at 102% RTP results in the highest calculated internal containment pressure of 55.7 psig, which is below the internal design pressure of 60 psig. The postulated DBAs are analyzed assuming degraded containment Engineered Safety Feature (ESF) systems (i.e., assuming the loss of one ESF bus, which is the worst case single active failure, resulting in one train of the Containment Spray System and one train of the Containment Cooling System being rendered inoperable). It is this maximum containment pressure that is used to ensure that the licensing basis dose limitations are met.

The initial pressure condition used in the containment analysis was [14.7] psia ([0.0] psig). This resulted in a maximum peak pressure from an MSLB of [55.7] psig. The LCO limit of [1.5] psig ensures that, in the event of an accident, the maximum accident design pressure for containment, [60] psig, is not exceeded. If an MSLB occurred while the containment internal pressure was at the LCO value of [1.5] psig, a total pressure of [57.3] psig would result. This value is still below the design value of [60] psig. The containment was also designed for an internal pressure equal to [5.0] psig below external pressure in order to withstand the resultant pressure drop from an accidental actuation of the

BASES

APPLICABLE SAFETY ANALYSES (continued)

Containment Spray System. The LCO limit of [-0.3] psig ensures that operation within the design limit of [-0.5] psig is maintained. The maximum calculated external pressure that would occur as a result of an inadvertent actuation of the Containment Spray System is [2.8] psig.

Containment pressure satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

Maintaining containment pressure less than or equal to the LCO upper pressure limit ensures that, in the event of a DBA, the resultant peak containment accident pressure will remain below the containment design pressure. Maintaining containment pressure greater than or equal to the LCO lower pressure limit ensures that the containment will not exceed the design negative pressure differential following the inadvertent actuation of the Containment Spray System.

APPLICABILITY

In MODES 1, 2, 3, and 4, a DBA could cause a release of radioactive material to containment. Since maintaining containment pressure within limits is essential to ensure initial conditions assumed in the accident analysis are maintained, the LCO is applicable in MODES 1, 2, 3, and 4.

In MODES 5 and 6, the probability and consequences of these events are reduced due to the pressure and temperature limitations of these MODES. Therefore, maintaining containment pressure within the limits of the LCO is not required in MODE 5 or 6.

ACTIONS

A.1

When containment pressure is not within the limits of the LCO, containment pressure must be restored to within these limits within 1 hour. The Required Action is necessary to return operation to within the bounds of the containment analysis. The 1 hour Completion Time is consistent with the ACTIONS of LCO 3.6.1, "Containment," which requires that containment be restored to OPERABLE status within 1 hour.

B.1 and B.2

If containment pressure cannot be restored to within limits within the required Completion Time, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 5 within 36 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

BASES

SURVEILLANCE REQUIREMENTS	SR 3.6.4A.1 Verifying that containment pressure is within limits ensures that operation remains within the limits assumed in the accident analysis. The 12 hour Frequency of this SR was developed after taking into consideration operating experience related to trending of containment pressure variations during the applicable MODES. Furthermore, the 12 hour Frequency is considered adequate in view of other indications available in the control room, including alarms, to alert the operator to an abnormal containment pressure condition.
REFERENCES	None.

B 3.6 CONTAINMENT SYSTEMS

B 3.6.4B Containment Pressure (Dual)

BASES

BACKGROUND	The containment pressure is limited, during normal operation, to preserve the initial conditions assumed in the accident analyses for a loss of coolant accident (LOCA) or main steam line break (MSLB). These limits also prevent the containment pressure from exceeding the containment design negative pressure differential, with respect to the outside atmosphere, in the event of inadvertent actuation of the Containment Spray System. Containment pressure is a process variable that is monitored and controlled. The containment pressure limits are derived from the input conditions used in the containment functional analyses and the containment structure external pressure analysis. Should operation occur outside these limits coincident with a Design Basis Accident (DBA), post accident containment pressures could exceed calculated values.
APPLICABLE SAFETY ANALYSES	Containment internal pressure is an initial condition used in the DBA analyses to establish the maximum peak containment internal pressure. The limiting DBAs considered for determining the maximum containment internal pressure (P_a) are the LOCA and MSLB. An MSLB at 75% RTP results in the highest calculated internal containment pressure of 42.3 psig, which is below the internal design pressure of 44 psig. The postulated DBAs are analyzed assuming degraded containment Engineered Safety Feature (ESF) systems (i.e., assuming the loss of one ESF bus, which is the worst case single active failure, resulting in one train of the Containment Spray System and one train of the Containment Cooling System being rendered inoperable). It is this maximum containment pressure that is used to ensure that the licensing basis dose limitations are met. The initial pressure condition used in the containment analysis was [14.7] psig. The maximum containment pressure resulting from the limiting DBA, [42.3] psig, does not exceed the containment design pressure, [44] psig. The containment was also designed for an internal pressure equal to [0.65] psid below external pressure to withstand the resultant pressure drop from an accidental actuation of the Containment Spray System. The LCO limit of [27] inches of water ensures that operation within the design limit of [-0.65] psid is maintained. The maximum calculated differential pressure that would occur as a result of an inadvertent actuation of the Containment Spray System is [0.49] psid. Containment pressure satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO	Maintaining containment pressure less than or equal to the LCO upper pressure limit ensures that, in the event of a DBA, the resultant peak containment accident pressure will remain below the containment design pressure. Maintaining containment pressure greater than or equal to the LCO lower pressure limit ensures the containment will not exceed the design negative differential pressure following the inadvertent actuation of the Containment Spray System.
APPLICABILITY	In MODES 1, 2, 3, and 4, a DBA could cause a release of radioactive material to containment. Since maintaining containment pressure within limits is essential to ensure initial conditions assumed in the accident analysis are maintained, the LCO is applicable in MODES 1, 2, 3, and 4. In MODES 5 and 6, the probability and consequences of these events are reduced due to the pressure and temperature limitations of these MODES.
ACTIONS	<u>A.1</u> When containment pressure is not within the limits of the LCO, containment pressure must be restored to within these limits within 1 hour. The Required Action is necessary to return operation to within the bounds of the containment analysis. The 1 hour Completion Time is consistent with the ACTIONS of LCO 3.6.1, "Containment," which requires that containment be restored to OPERABLE status within 1 hour. <u>B.1 and B.2</u> If containment pressure cannot be restored to within limits within the required Completion Time, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 5 within 36 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.
SURVEILLANCE REQUIREMENTS	<u>SR 3.6.4B.1</u> Verifying that containment pressure is within limits ensures that facility operation remains within the limits assumed in the containment analysis. The 12 hour Frequency of this SR was developed after taking into consideration operating experience related to trending of containment pressure variations during the applicable MODES. Furthermore, the 12 hour Frequency is considered adequate in view of other indications available in the control room, including alarms, to alert the operator to an abnormal containment pressure condition.

BASES

REFERENCES None.

B 3.6 CONTAINMENT SYSTEMS

B 3.6.5 Containment Air Temperature (Atmospheric and Dual)

BASES

BACKGROUND	The containment structure serves to contain radioactive material that may be released from the reactor core following a Design Basis Accident (DBA). The containment average air temperature is limited during normal operation to preserve the initial conditions assumed in the accident analyses for a loss of coolant accident (LOCA) or main steam line break (MSLB). The containment average air temperature limit is derived from the input conditions used in the containment functional analyses and the containment structure external pressure analyses. This LCO ensures that initial conditions assumed in the analysis of containment response to a DBA are not violated during unit operations. The total amount of energy to be removed from containment by the Containment Spray and Cooling systems during post accident conditions is dependent on the energy released to the containment due to the event, as well as the initial containment temperature and pressure. The higher the initial temperature, the more energy that must be removed, resulting in a higher peak containment pressure and temperature. Exceeding containment design pressure may result in leakage greater than that assumed in the accident analysis (Ref. 1). Operation with containment temperature in excess of the LCO limit violates an initial condition assumed in the accident analysis.
APPLICABLE SAFETY ANALYSES	Containment average air temperature is an initial condition used in the DBA analyses that establishes the containment environmental qualification operating envelope for both pressure and temperature. The limit for containment average air temperature ensures that operation is maintained within the assumptions used in the DBA analysis for containment. The accident analyses and evaluations considered both LOCAs and MSLBs for determining the maximum peak containment pressures and temperatures. The worst case MSLB generates larger mass and energy releases than the worst case LOCA. Thus, the MSLB event bounds the LOCA event from the containment peak pressure and temperature standpoint. The initial pre-accident temperature inside containment was assumed to be [120]°F (Ref. 2). [For atmospheric containment, the initial containment average air temperature condition of [120]°F resulted in a maximum vapor temperature in containment of [413]°F. The temperature of the

BASES

APPLICABLE SAFETY ANALYSES (continued)

containment steel liner and concrete structure reach approximately 230°F and 220°F, respectively. The containment average air temperature limit of [120]°F ensures that, in the event of an accident, the maximum design temperature for containment, [300]°F, is not exceeded. The consequence of exceeding this design temperature may be the potential for degradation of the containment structure under accident loads.

For dual containment, the initial containment condition of [120]°F resulted in a maximum vapor temperature in containment of [413.5]°F. The temperature of the containment steel pressure vessel also reaches approximately [413.5]°F. The containment average temperature limit of [120]°F ensures that, in the event of an accident, the maximum design temperature for containment of [269.3]°F during LOCA conditions and [413.5]°F during MSLB conditions is not exceeded. The consequences of exceeding this design temperature may be the potential for degradation of the containment structure under accident loads.]

Containment average air temperature satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

During a DBA, with an initial containment average air temperature less than or equal to the LCO temperature limit, the resultant accident temperature profile assures that the containment structural temperature is maintained below its design temperature and that required safety related equipment will continue to perform its function.

APPLICABILITY

In MODES 1, 2, 3, and 4, a DBA could cause a release of radioactive material to containment. In MODES 5 and 6, the probability and consequences of these events are reduced due to the pressure and temperature limitations of these MODES. Therefore, maintaining containment average air temperature within the limit is not required in MODE 5 or 6.

ACTIONS

A.1

When containment average air temperature is not within the limit of the LCO, it must be restored to within limit within 8 hours. This Required Action is necessary to return operation to within the bounds of the containment analysis. The 8 hour Completion Time is acceptable considering the sensitivity of the analysis to variations in this parameter and provides sufficient time to correct minor problems.

BASES

ACTIONS (continued)

B.1 and B.2

If the containment average air temperature cannot be restored to within its limit within the required Completion Time, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 5 within 36 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.6.5.1

Verifying that containment average air temperature is within the LCO limit ensures that containment operation remains within the limit assumed for the containment analyses. In order to determine the containment average air temperature, an arithmetic average is calculated using measurements taken at locations within the containment selected to provide a representative sample of the overall containment atmosphere. The 24 hour Frequency of this SR is considered acceptable based on the observed slow rates of temperature increase within containment as a result of environmental heat sources (due to the large volume of containment). Furthermore, the 24 hour Frequency is considered adequate in view of other indications available in the control room, including alarms, to alert the operator to an abnormal containment temperature condition.

REFERENCES

1. FSAR, Section [ ].
2. FSAR, Section [ ].

B 3.6 CONTAINMENT SYSTEMS

B 3.6.6A Containment Spray and Cooling Systems (Atmospheric and Dual) (Credit taken for iodine removal by the Containment Spray System)

BASES

BACKGROUND

The Containment Spray and Containment Cooling systems provide containment atmosphere cooling to limit post accident pressure and temperature in containment to less than the design values. Reduction of containment pressure and the iodine removal capability of the spray reduce the release of fission product radioactivity from containment to the environment, in the event of a Design Basis Accident (DBA), to within limits. The Containment Spray and Containment Cooling systems are designed to the requirements of 10 CFR 50, Appendix A, GDC 38, "Containment Heat Removal," GDC 39, "Inspection of Containment Heat Removal Systems," GDC 40, "Testing of Containment Heat Removal Systems," GDC 41, "Containment Atmosphere Cleanup," GDC 42, "Inspection of Containment Atmosphere Cleanup Systems," and GDC 43, "Testing of Containment Atmosphere Cleanup Systems" (Ref. 1), or other documents that were appropriate at the time of licensing (identified on a unit specific basis).

The Containment Cooling System and Containment Spray System are Engineered Safety Feature (ESF) systems. They are designed to ensure that the heat removal capability required during the post accident period can be attained. The Containment Spray System and the Containment Cooling System provide redundant methods to limit and maintain post accident conditions to less than the containment design values.

Containment Spray System

The Containment Spray System consists of two separate trains of equal capacity, each capable of meeting the design bases. Each train includes a containment spray pump, spray headers, nozzles, valves, and piping. Each train is powered from a separate ESF bus. The refueling water tank (RWT) supplies borated water to the containment spray during the injection phase of operation. In the recirculation mode of operation, containment spray pump suction is transferred from the RWT to the containment sump(s).

The Containment Spray System provides a spray of cold borated water mixed with sodium hydroxide from the spray additive tank into the upper regions of containment to reduce containment pressure and temperature and to reduce the concentration of fission products in the containment atmosphere during a DBA. The RWT solution temperature is an

BASES

BACKGROUND (continued)

important factor in determining the heat removal capability of the Containment Spray System during the injection phase. In the recirculation mode of operation, heat is removed from the containment sump water by the shutdown cooling heat exchangers. Each train of the Containment Spray System provides adequate spray coverage to meet 50% of the system design requirements for containment heat removal and 100% of the iodine removal design bases.

The Spray Additive System injects a hydrazine (N_2H_4) solution into the spray. The resulting alkaline pH of the spray enhances its ability to scavenge fission products from the containment atmosphere. The N_2H_4 added to the spray also ensures an alkaline pH for the solution recirculated in the containment sump. The alkaline pH of the containment sump water minimizes the evolution of iodine and minimizes the occurrence of chloride and caustic stress corrosion on mechanical systems and components exposed to the fluid.

The Containment Spray System is actuated either automatically by a containment High-High pressure signal coincident with a safety injection actuation signal (SIAS) or manually. An automatic actuation opens the containment spray pump discharge valves, starts the two Containment Spray System pumps, and begins the injection phase. The containment spray header isolation valves open upon a containment spray actuation signal. A manual actuation of the Containment Spray System is available on the main control board to begin the same sequence. The injection phase continues until an RWT level Low signal is received. The Low level for the RWT generates a recirculation actuation signal that aligns valves from the containment spray pump suction to the containment sump. The Containment Spray System in recirculation mode maintains an equilibrium temperature between the containment atmosphere and the recirculated sump water. Operation of the Containment Spray System in the recirculation mode is controlled by the operator in accordance with the emergency operating procedures.

Containment Cooling System

Two trains of containment cooling, each of sufficient capacity to supply 50% of the design cooling requirement, are provided. Two trains with two fan units each are supplied with cooling water from a separate train of service water cooling. All four fans are required to furnish the design cooling capacity. Air is drawn into the coolers through the fans and discharged to the steam generator compartments and pressurizer compartment.

BASES

BACKGROUND (continued)

In post accident operation following a containment cooling actuation signal (CCAS), all four Containment Cooling System fans are designed to start automatically in slow speed. Cooling is shifted from the chilled water cooled coils to the service water cooled coils. The temperature of the service water is an important factor in the heat removal capability of the fan units.

APPLICABLE SAFETY ANALYSES

The Containment Spray System and Containment Cooling System limit the temperature and pressure that could be experienced following a DBA. The limiting DBAs considered relative to containment temperature and pressure are the loss of coolant accident (LOCA) and the main steam line break (MSLB). The DBA LOCA and MSLB are analyzed using computer codes designed to predict the resultant containment pressure and temperature transients. No DBAs are assumed to occur simultaneously or consecutively. The postulated DBAs are analyzed with regard to containment ESF systems, assuming the loss of one ESF bus, which is the worst case single active failure, resulting in one train of the Containment Spray System and one train of the Containment Cooling System being rendered inoperable.

The analysis and evaluation show that under the worst case scenario, the highest peak containment pressure is [55.7] psig (experienced during an MSLB). The analysis shows that the peak containment vapor temperature is [413]°F (experienced during an MSLB). Both results are within the design. (See the Bases for Specifications 3.6.4A and 3.6.4B, "Containment Pressure," and 3.6.5, "Containment Air Temperature," for a detailed discussion.) The analyses and evaluations assume a power level of [102]% RTP, one containment spray train and one containment cooling train operating, and initial (pre-accident) conditions of [120]°F and [14.7] psia. The analyses also assume a response time delayed initiation in order to provide a conservative calculation of peak containment pressure and temperature responses.

The effect of an inadvertent containment spray actuation has been analyzed. An inadvertent spray actuation reduces the containment pressure to [-2.8] psig due to the sudden cooling effect in the interior of the air tight containment. Additional discussion is provided in the Bases for Specifications 3.6.4A, 3.6.4B, and 3.6.12, "Vacuum Relief Valves."

BASES

APPLICABLE SAFETY ANALYSES (continued)

The modeled Containment Spray System actuation from the containment analysis is based upon a response time associated with exceeding the containment High-High pressure setpoint coincident with an SIAS to achieve full flow through the containment spray nozzles. The Containment Spray System total response time of [60] seconds includes diesel generator startup (for loss of offsite power), block loading of equipment, containment spray pump startup, and spray line filling (Ref. 2).

The performance of the containment cooling train for post accident conditions is given in Reference 3. The result of the analysis is that each train can provide 50% of the required peak cooling capacity during the post accident condition. The train post accident cooling capacity under varying containment ambient conditions, required to perform the accident analyses, is also shown in Reference 4.

The modeled Containment Cooling System actuation from the containment analysis is based upon the unit specific response time associated with exceeding the CCAS to achieve full Containment Cooling System air and safety grade cooling water flow.

The Containment Spray System and the Containment Cooling System satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

During a DBA, a minimum of two containment cooling trains or two containment spray trains, or one of each, is required to maintain the containment peak pressure and temperature below the design limits (Ref. 5). Additionally, one containment spray train is also required to remove iodine from the containment atmosphere and maintain concentrations below those assumed in the safety analysis. To ensure that these requirements are met, two containment spray trains and two containment cooling units must be OPERABLE. Therefore, in the event of an accident, the minimum requirements are met, assuming that the worst case single active failure occurs.

Each Containment Spray System includes a spray pump, spray headers, nozzles, valves, piping, instruments, and controls to ensure an OPERABLE flow path capable of taking suction from the RWT upon an ESF actuation signal and automatically transferring suction to the containment sump.

Each Containment Cooling System includes demisters, cooling coils, dampers, fans, instruments, and controls to ensure an OPERABLE flow path.

BASES

APPLICABILITY

In MODES 1, 2, 3, and 4, a DBA could cause a release of radioactive material to containment and an increase in containment pressure and temperature, requiring the operation of the containment spray trains and containment cooling trains.

In MODES 5 and 6, the probability and consequences of these events are reduced due to the pressure and temperature limitations of these MODES. Thus, the Containment Spray and Containment Cooling systems are not required to be OPERABLE in MODES 5 and 6.

ACTIONS

A.1

-----------------------------------REVIEWER'S NOTE-----------------------------------
Utilization of the 7 day Completion Time for Required Action A.1 is dependent on the licensee adopting CE NPSD-1045-A (Ref. 6) and meeting the requirements of the Topical Report and the associated Safety Evaluation. Otherwise, a 72 hour Completion Time applies.

With one containment spray train inoperable, the inoperable containment spray train must be restored to OPERABLE status within [7] days. In this Condition, the remaining OPERABLE spray and cooling trains are adequate to perform the iodine removal and containment cooling functions. The [7] day Completion Time takes into account the redundant heat removal capability afforded by the Containment Spray System, reasonable time for repairs, and the findings of Ref. 6.

B.1 and B.2

If the inoperable containment spray train cannot be restored to OPERABLE status within the required Completion Time, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 5 within 84 hours. The allowed Completion Time of 6 hours is reasonable, based on operating experience, to reach MODE 3 from full power conditions in an orderly manner and without challenging plant systems. The extended interval to reach MODE 5 allows additional time for the restoration of the containment spray train and is reasonable when considering that the driving force for a release of radioactive material from the Reactor Coolant System is reduced in MODE 3.

BASES

ACTIONS (continued)

C.1

With one required containment cooling train inoperable, the inoperable containment cooling train must be restored to OPERABLE status within 7 days. The remaining OPERABLE containment spray and cooling components provide iodine removal capabilities and are capable of providing at least 100% of the heat removal needs after an accident. The 7 day Completion Time was developed taking into account the redundant heat removal capabilities afforded by combinations of the Containment Spray System and Containment Cooling System and the low probability of a DBA occurring during this period.

D.1 and D.2

With one containment spray and one containment cooling train inoperable, one of the required containment cooling trains must be restored to OPERABLE status within 72 hours. The components in this degraded condition provide iodine removal capabilities and are capable of providing at least 100% of the heat removal needs after an accident. The 72 hour Completion Time was developed taking into account the redundant heat removal capabilities afforded by combinations of the Containment Spray System and Containment Cooling System, the iodine removal function of the Containment Spray System, and the low probability of a DBA occurring during this period.

E.1

With two required containment cooling trains inoperable, one of the required containment cooling trains must be restored to OPERABLE status within 72 hours. The components in this degraded condition provide iodine removal capabilities and are capable of providing at least 100% of the heat removal needs after an accident. The 72 hour Completion Time was developed taking into account the redundant heat removal capabilities afforded by combinations of the Containment Spray System and Containment Cooling System, the iodine removal function of the Containment Spray System, and the low probability of a DBA occurring during this period.

BASES

ACTIONS (continued)

F.1 and F.2

If the Required Actions and associated Completion Times of Condition C, D, or E of this LCO are not met, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 5 within 36 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

G.1

With two containment spray trains or any combination of three or more Containment Spray System and Containment Cooling System trains inoperable, the unit is in a condition outside the accident analysis. Therefore, LCO 3.0.3 must be entered immediately.

SURVEILLANCE REQUIREMENTS

SR 3.6.6A.1

Verifying the correct alignment for manual, power operated, and automatic valves in the containment spray flow path provides assurance that the proper flow paths will exist for Containment Spray System operation. This SR does not apply to valves that are locked, sealed, or otherwise secured in position since these were verified to be in the correct position prior to being secured. This SR also does not apply to valves that cannot be inadvertently misaligned, such as check valves. This SR does not require any testing or valve manipulation. Rather, it involves verifying that those valves outside containment and capable of potentially being mispositioned are in the correct position.

SR 3.6.6A.2

Operating each containment cooling train fan unit for ≥ 15 minutes ensures that all trains are OPERABLE and that all associated controls are functioning properly. It also ensures that blockage, fan or motor failure, or excessive vibration can be detected and corrective action taken. The 31 day Frequency of this SR was developed considering the known reliability of the fan units and controls, the two train redundancy available, and the low probability of a significant degradation of the containment cooling train occurring between surveillances and has been shown to be acceptable through operating experience.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.6.6A.3

Verifying a service water flow rate of ≥ [2000] gpm to each cooling unit provides assurance that the design flow rate assumed in the safety analyses will be achieved (Ref. 2). Also considered in selecting this Frequency were the known reliability of the Cooling Water System, the two train redundancy, and the low probability of a significant degradation of flow occurring between surveillances.

[SR 3.6.6A.4

Verifying that the containment spray header piping is full of water to the [100] ft level minimizes the time required to fill the header. This ensures that spray flow will be admitted to the containment atmosphere within the time frame assumed in the containment analysis. The 31 day Frequency is based on the static nature of the fill header and the low probability of a significant degradation of water level in the piping occurring between surveillances.]

SR 3.6.6A.5

Verifying that each containment spray pump's developed head at the flow test point is greater than or equal to the required developed head ensures that spray pump performance has not degraded during the cycle. Flow and differential pressure are normal tests of centrifugal pump performance required by the ASME Code (Ref. 7). Since the containment spray pumps cannot be tested with flow through the spray headers, they are tested on recirculation flow. This test confirms one point on the pump design curve and is indicative of overall performance. Such inservice inspections confirm component OPERABILITY, trend performance, and detect incipient failures by indicating abnormal performance. The Frequency of this SR is in accordance with the Inservice Testing Program.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.6.6A.6 and SR 3.6.6A.7

These SRs verify that each automatic containment spray valve actuates to its correct position and that each containment spray pump starts upon receipt of an actual or simulated actuation signal. This Surveillance is not required for valves that are locked, sealed, or otherwise secured in the required position under administrative controls. The [18] month Frequency is based on the need to perform these Surveillances under the conditions that apply during a plant outage and the potential for an unplanned transient if the Surveillances were performed with the reactor at power. Operating experience has shown that these components usually pass the Surveillances when performed at the [18] month Frequency. Therefore, the Frequency was concluded to be acceptable from a reliability standpoint.

The surveillance of containment sump isolation valves is also required by SR 3.5.2.5. A single surveillance may be used to satisfy both requirements.

SR 3.6.6A.8

This SR verifies that each containment cooling train actuates upon receipt of an actual or simulated actuation signal. The [18] month Frequency is based on engineering judgment and has been shown to be acceptable through operating experience. See SR 3.6.6A.6 and SR 3.6.6A.7, above, for further discussion of the basis for the [18] month Frequency.

SR 3.6.6A.9

With the containment spray inlet valves closed and the spray header drained of any solution, low pressure air or smoke can be blown through test connections. Performance of this SR demonstrates that each spray nozzle is unobstructed and provides assurance that spray coverage of the containment during an accident is not degraded. Due to the passive design of the nozzle, a test at [the first refueling and at] 10 year intervals is considered adequate to detect obstruction of the spray nozzles.

BASES

REFERENCES

1. 10 CFR 50, Appendix A, GDC 38, GDC 39, GDC 40, GDC 41, GDC 42, and GDC 43.
2. FSAR, Section [ ].
3. FSAR, Section [ ].
4. FSAR, Section [ ].
5. FSAR, Section [ ].
6. CE NPSD-1045-A, “CEOG Joint Application Report for Modification to the Containment Spray System Technical Specifications," March 2000.
7. ASME Code for Operation and Maintenance of Nuclear Power Plants.

B 3.6 CONTAINMENT SYSTEMS

B 3.6.6B Containment Spray and Cooling Systems (Atmospheric and Dual) (Credit not taken for iodine removal by the Containment Spray System)

BASES

BACKGROUND

The Containment Spray and Containment Cooling systems provide containment atmosphere cooling to limit post accident pressure and temperature in containment to less than the design values. Reduction of containment pressure reduces the release of fission product radioactivity from containment to the environment, in the event of a Design Basis Accident (DBA). The Containment Spray and Containment Cooling systems are designed to the requirements of 10 CFR 50, Appendix A, GDC 38, "Containment Heat Removal," GDC 39, "Inspection of Containment Heat Removal Systems," GDC 40, "Testing of Containment Heat Removal Systems," GDC 41, "Containment Atmosphere Cleanup," GDC 42, "Inspection of Containment Atmosphere Cleanup Systems," and GDC 43, "Testing of Containment Atmosphere Cleanup Systems" (Ref. 1), or other documents that were appropriate at the time of licensing (identified on a unit specific basis).

The Containment Cooling System and Containment Spray System are Engineered Safety Feature (ESF) systems. They are designed to ensure that the heat removal capability required during the post accident period can be attained. The Containment Spray System and the Containment Cooling System provide redundant methods to limit and maintain post accident conditions to less than the containment design values.

<u>Containment Spray System</u>

The Containment Spray System consists of two separate trains of equal capacity, each capable of meeting the design bases. Each train includes a containment spray pump, spray headers, nozzles, valves, and piping. Each train is powered from a separate ESF bus. The refueling water tank (RWT) supplies borated water to the containment spray during the injection phase of operation. In the recirculation mode of operation, containment spray pump suction is transferred from the RWT to the containment sump(s).

The Containment Spray System provides a spray of cold borated water into the upper regions of containment to reduce the containment pressure and temperature during a DBA. The RWT solution temperature is an important factor in determining the heat removal capability of the Containment Spray System during the injection phase. In the

BASES

BACKGROUND (continued)

recirculation mode of operation, heat is removed from the containment sump water by the shutdown cooling heat exchangers. Each train of the Containment Spray System provides adequate spray coverage to meet 50% of the system design requirements for containment heat removal.

The Containment Spray System is actuated either automatically by a containment High-High pressure signal coincident with a safety injection actuation signal (SIAS) or manually. An automatic actuation opens the containment spray pump discharge valves, starts the two containment spray pumps, and begins the injection phase. The containment spray header isolation valves open on a containment spray actuation signal. A manual actuation of the Containment Spray System is available on the main control board to begin the same sequence. The injection phase continues until an RWT level Low signal is received. The Low level signal for the RWT generates a recirculation actuation signal that aligns valves from the containment spray pump suction to the containment sump. The Containment Spray System in recirculation mode maintains an equilibrium temperature between the containment atmosphere and the recirculated sump water. Operation of the Containment Spray System in the recirculation mode is controlled by the operator in accordance with the emergency operating procedures.

Containment Cooling System

Two trains of containment cooling, each of sufficient capacity to supply 50% of the design cooling requirements, are provided. Two trains with two fan units each are supplied with cooling water from a separate train of service water. All four fans are required to furnish the design cooling capacity. Air is drawn into the coolers through the fan and discharged to the steam generator compartments and pressurizer compartments.

In post accident operation following a containment cooling actuation signal (CCAS), all four Containment Cooling System fans are designed to start automatically in slow speed, if not already running. Cooling is shifted from the chilled water cooled coils to the service water cooled coils. The temperature of the service water is an important factor in the heat removal capability of the fan units.

APPLICABLE SAFETY ANALYSES

The Containment Spray System and Containment Cooling System limit the temperature and pressure that could be experienced following a DBA. The limiting DBAs considered relative to containment temperature and pressure are the loss of coolant accident (LOCA) and the main steam line break (MSLB). The DBA LOCA and MSLB are analyzed using

BASES

APPLICABLE SAFETY ANALYSES (continued)

computer codes designed to predict the resultant containment pressure and temperature transients. No DBAs are assumed to occur simultaneously or consecutively. The postulated DBAs are analyzed, in regard to containment ESF systems, assuming the loss of one ESF bus, which is the worst case single active failure, resulting in one train of the Containment Spray System and one train of Containment Cooling System being rendered inoperable.

The analysis and evaluation show that under the worst case scenario, the highest peak containment pressure is [55.7] psig (experienced during an MSLB). The analysis shows that the peak containment vapor temperature is [414]°F (experienced during an MSLB). Both results are within the intent of the design basis. (See the Bases for Specifications 3.6.4A and 3.6.4B, "Containment Pressure," and 3.6.5, "Containment Air Temperature," for a detailed discussion.) The analyses and evaluations assume a power level of [102]% RTP, one containment spray train and one containment cooling train operating, and initial (pre-accident) conditions of [120]°F and [14.7] psia. The analyses also assume a response time delayed initiation in order to provide conservative peak calculated containment pressure and temperature responses.

The effect of an inadvertent containment spray actuation has been analyzed. An inadvertent spray actuation reduces the containment pressure to [-2.8] psig due to the sudden cooling effect in the interior of the air tight containment. Additional discussion is provided in the Bases for Specifications 3.6.4A, 3.6.4B, and 3.6.12, "Vacuum Relief Valves."

The modeled Containment Spray System actuation from the containment analysis is based on a response time associated with exceeding the containment High-High pressure setpoint coincident with an SIAS to achieve full flow through the containment spray nozzles. The Containment Spray System total response time of [60] seconds includes diesel generator startup (for loss of offsite power), block loading of equipment, containment spray pump startup, and spray line filling (Ref. 2).

The performance of the containment cooling train for post accident conditions is given in Reference 3. The result of the analysis is that each train can provide 50% of the required peak cooling capacity during the post accident condition. The train post accident cooling capacity under varying containment ambient conditions, required to perform the accident analyses, is also shown in Reference [4].

BASES

APPLICABLE SAFETY ANALYSES (continued)

The modeled Containment Cooling System actuation from the containment analysis is based on the unit specific response time associated with exceeding the CCAS to achieve full Containment Cooling System air and safety grade cooling water flow.

The Containment Spray System and the Containment Cooling System satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

During a DBA, a minimum of two containment cooling trains or two containment spray trains, or one of each, is required to maintain the containment peak pressure and temperature below the design limits (Ref. 5). To ensure that these requirements are met, two containment spray trains and two containment cooling units must be OPERABLE. Therefore, in the event of an accident, the minimum requirements are met, assuming the worst case single active failure occurs.

Each Containment Spray System typically includes a spray pump, spray headers, nozzles, valves, piping, instruments, and controls to ensure an OPERABLE flow path capable of taking suction from the RWT upon an ESF actuation signal and automatically transferring suction to the containment sump.

Each Containment Cooling System typically includes demisters, cooling coils, dampers, fans, instruments, and controls to ensure an OPERABLE flow path.

APPLICABILITY

In MODES 1, 2, 3, and 4, a DBA could cause a release of radioactive material to containment and an increase in containment pressure and temperature requiring the operation of the containment spray trains and containment cooling trains.

In MODES 5 and 6, the probability and consequences of these events are reduced due to the pressure and temperature limitations of these MODES. Thus, the Containment Spray and Containment Cooling systems are not required to be OPERABLE in MODES 5 and 6.

ACTIONS

A.1

With one containment spray train inoperable, the inoperable containment spray train must be restored to OPERABLE status within 7 days. The components in this degraded condition are capable of providing greater than 100% of the heat removal needs (for the condition of one containment spray train inoperable) after an accident. The 7 day

BASES

ACTIONS (continued)

Completion Time was developed taking into account the redundant heat removal capabilities afforded by combinations of the Containment Spray System and Containment Cooling System and the low probability of a DBA occurring during this period.

B.1

With one required containment cooling train inoperable, the inoperable containment cooling train must be restored to OPERABLE status within 7 days. The components in this degraded condition are capable of providing greater than 100% of the heat removal needs (for the condition of one containment cooling train inoperable) after an accident. The 7 day Completion Time was developed based on the same reasons as those for Required Action A.1.

C.1

With two required containment spray trains inoperable, one of the required containment spray trains must be restored to OPERABLE status within 72 hours. The components in this degraded condition are capable of providing greater than 100% of the heat removal needs after an accident. The 72 hour Completion Time was developed taking into account the redundant heat removal capabilities afforded by combinations of the Containment Spray System and Containment Cooling System and the low probability of a DBA occurring during this period.

D.1 and D.2

With one required containment spray train inoperable and one of the required containment cooling trains inoperable, the inoperable containment spray train or the inoperable containment cooling train must be restored to OPERABLE status within 72 hours. The components in this degraded condition are capable of providing at least 100% of the heat removal needs after an accident. The 72 hour Completion Time was developed based on the same reasons as those for Required Action C.1.

BASES

ACTIONS (continued)

E.1

With two containment cooling trains inoperable, one of the required containment cooling trains must be restored to OPERABLE status within 72 hours. The components in this degraded condition are capable of providing greater than 100% of the heat removal needs after an accident. The 72 hour Completion Time was developed based on the same reasons as those for Required Action C.1.

F.1 and F.2

If any of the Required Actions and associated Completion Times of this LCO are not met, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 5 within 36 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

G.1

With any combination of three or more Containment Spray System and Containment Cooling System trains inoperable, the unit is in a condition outside the accident analysis. Therefore, LCO 3.0.3 must be entered immediately.

SURVEILLANCE REQUIREMENTS

SR 3.6.6B.1

Verifying the correct alignment for manual, power operated, and automatic valves, excluding check valves, in the Containment Spray System provides assurance that the proper flow path exists for Containment Spray System operation. This SR also does not apply to valves that are locked, sealed, or otherwise secured in position since these were verified to be in the correct positions prior to being secured. This SR also does not apply to valves that cannot be inadvertently misaligned, such as check valves. This SR does not require any testing or valve manipulation. Rather, it involves verification that those valves outside containment and capable of potentially being mispositioned, are in the correct position.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.6.6B.2

Operating each containment cooling train fan unit for ≥ 15 minutes ensures that all trains are OPERABLE and that all associated controls are functioning properly. It also ensures that blockage, fan or motor failure, or excessive vibration can be detected for corrective action. The 31 day Frequency was developed considering the known reliability of the fan units and controls, the two train redundancy available, and the low probability of a significant degradation of the containment cooling train occurring between surveillances.

SR 3.6.6B.3

Verifying a service water flow rate of ≥ [2000] gpm to each cooling unit provides assurance the design flow rate assumed in the safety analyses will be achieved (Ref. 2). Also considered in selecting this Frequency were the known reliability of the cooling water system, the two train redundancy, and the low probability of a significant degradation of flow occurring between surveillances.

[SR 3.6.6B.4

Verifying the containment spray header is full of water to the [100] ft level minimizes the time required to fill the header. This ensures that spray flow will be admitted to the containment atmosphere within the time frame assumed in the containment analysis. The 31 day Frequency is based on the static nature of the fill header and the low probability of a significant degradation of the water level in the piping occurring between surveillances.]

SR 3.6.6B.5

Verifying that each containment spray pump's developed head at the flow test point is greater than or equal to the required developed head ensures that spray pump performance has not degraded during the cycle. Flow and differential pressure are normal tests of centrifugal pump performance required by the ASME Code (Ref. 6). Since the containment spray pumps cannot be tested with flow through the spray headers, they are tested on recirculation flow. This test confirms one point on the pump

BASES

SURVEILLANCE REQUIREMENTS (continued)

design curve and is indicative of overall performance. Such inservice inspections confirm component OPERABILITY, trend performance, and detect incipient failures by indicating abnormal performance. The Frequency of this SR is in accordance with the Inservice Testing Program.

SR 3.6.6B.6 and SR 3.6.6B.7

These SRs verify each automatic containment spray valve actuates to its correct position and that each containment spray pump starts upon receipt of an actual or simulated actuation signal. This Surveillance is not required for valves that are locked, sealed, or otherwise secured in the required position under administrative controls. The [18] month Frequency is based on the need to perform these Surveillances under the conditions that apply during a plant outage and the potential for an unplanned transient if the Surveillances were performed with the reactor at power. Operating experience has shown that these components usually pass the Surveillances when performed at the [18] month Frequency. Therefore, the Frequency was concluded to be acceptable from a reliability standpoint.

The surveillance of containment sump isolation valves is also required by SR 3.5.2.5. A single surveillance may be used to satisfy both requirements.

SR 3.6.6B.8

This SR verifies each containment cooling train actuates upon receipt of an actual or simulated actuation signal. The [18] month Frequency is based on engineering judgment and has been shown to be acceptable through operating experience. See SR 3.6.6B.6 and SR 3.6.6B.7, above, for further discussion of the basis for the [18] month Frequency.

SR 3.6.6B.9

With the containment spray inlet valves closed and the spray header drained of any solution, low pressure air or smoke can be blown through test connections. Performance of this SR demonstrates that each spray nozzle is unobstructed and provides assurance that spray coverage of the containment during an accident is not degraded. Due to the passive design of the nozzle, a test at [the first refueling and at] 10 year intervals is considered adequate to detect obstruction of the spray nozzles.

BASES

REFERENCES

1. 10 CFR 50, Appendix A, GDC 38, GDC 39, GDC 40, GDC 41, GDC 42, and GDC 43.

2. FSAR, Section [ ].

3. FSAR, Sections [ ].

4. FSAR, Section [ ].

5. FSAR, Section [ ].

6. ASME Code for Operation and Maintenance of Nuclear Power Plants.

B 3.6 CONTAINMENT SYSTEMS

B 3.6.7 Spray Additive System (Atmospheric and Dual)

BASES

BACKGROUND

The Spray Additive System is a subsystem of the Containment Spray System that assists in reducing the iodine fission product inventory in the containment atmosphere in the event of an accident such as a loss of coolant accident (LOCA).

The addition of a spray additive to the boric acid spray solution increases the pH of the spray solution and maintains the containment sump pH above 8.0 during the recirculation phase of an accident. An elevated pH is desired since it enhances the iodine removal capacity of the sprays and aids in the retention of iodine in the water in the containment sump.

The Spray Additive System consists of a single spray additive tank and two redundant 100% capacity trains. Each train contains a chemical addition pump, an injection valve, isolation valves, a flow meter, and a flow controller. Upon receipt of a containment spray actuation signal (CSAS), the chemical addition pumps start and the injection valves open in each redundant train. The spray additive is then injected into the Containment Spray System at the suction of the containment spray pumps at metered amounts corresponding to the individual containment spray pump discharge flow rate. The rate at which the spray additive is added is reduced when a recirculation actuation signal is generated and the Containment Spray System enters the recirculation mode of operation. The pH of the containment spray solution is maintained between 9.0 and 10.0 during the injection mode and between 8.0 and 9.0 in the recirculation mode. Upon reaching a Low-Low level in the spray chemical addition tank, the spray chemical addition pumps stop and the injection and isolation valves close (Ref. 1).

The Spray Additive System aids in reducing the iodine fission production inventory in the containment atmosphere.

APPLICABLE SAFETY ANALYSES

The Spray Additive System is essential to the effective removal of airborne iodine within containment following a Design Basis Accident (DBA).

Following the assumed release of radioactive materials into containment, the containment is assumed to leak at its design value following the accident.

BASES

APPLICABLE SAFETY ANALYSES (continued)

The DBA response time assumed for the Spray Additive System is the same as for the Containment Spray System and is discussed in the Bases for Specification 3.6.6, "Containment Spray and Cooling Systems."

The DBA analyses assume that one train of the Containment Spray System/Spray Additive System is inoperable and that the entire spray additive tank volume is added to the remaining Containment Spray System flow path.

During a LOCA, the iodine inventory released to the containment is considered to be released instantaneously and uniformly distributed in the containment free volume. The containment volume is made up of sprayed and unsprayed regions. The sprayed region is enveloped by direct spray and mixed by the dome air circulators and emergency fan coolers. Mixing between the sprayed and unsprayed regions is facilitated by the emergency fan coolers and condensation of steam by the sprays.

The Spray Additive System satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

The Spray Additive System is necessary to reduce the release of radioactive material to the environment in the event of a DBA. To be considered OPERABLE, the volume and concentration of the spray additive solution must be sufficient to maintain the pH of the spray solution between [9.0 and 10.0] in the injection mode and [8.0 and 9.0] in the recirculation mode. This pH range maximizes the effectiveness of the iodine removal mechanism, without introducing conditions that may induce caustic stress corrosion cracking of mechanical components.

During a LOCA, one Spray Additive System train is capable of providing 100% of the required iodine removal capacity. To ensure at least one train is available in the event of the limiting single failure, both trains must be maintained in an OPERABLE status.

APPLICABILITY

In MODES 1, 2, 3, and 4, a DBA could cause a release of radioactive material to containment requiring the operation of the Spray Additive System. The Spray Additive System assists in reducing the iodine fission product inventory prior to release to the environment.

In MODES 5 and 6, the probability and consequences of these events are reduced due to the pressure and temperature limitations in these MODES. Thus, the Spray Additive System is not required to be OPERABLE in MODES 5 and 6.

BASES

ACTIONS

A.1

With the Spray Additive System inoperable, the system must be restored to OPERABLE status within 72 hours. The pH adjustment of the containment spray flow for corrosion protection and iodine removal enhancement are reduced in this condition. The Containment Spray System would still be available and would remove some iodine from the containment atmosphere in the event of a DBA. The 72 hour Completion Time takes into account the redundant flow path capabilities and the low probability of the worst case DBA occurring during this period.

B.1 and B.2

If the Spray Additive System cannot be restored to OPERABLE status within the required Completion Time, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 5 within 84 hours. The allowed Completion Time of 6 hours is reasonable, based on operating experience, to reach MODE 3 from full power conditions in an orderly manner and without challenging plant systems. The extended interval to reach MODE 5 allows additional time for restoration of the Spray Additive System and is reasonable when considering the reduced pressure and temperature conditions in MODE 3 for the release of radioactive material from the Reactor Coolant System.

SURVEILLANCE REQUIREMENTS

SR 3.6.7.1

Verifying the correct alignment of Spray Additive System manual, power operated, and automatic valves in the spray additive flow path provides assurance that the system is able to provide additive to the Containment Spray System in the event of a DBA. This SR does not apply to valves that are locked, sealed, or otherwise secured in position since these valves were verified to be in the correct position prior to locking, sealing, or securing. This SR does not require any testing or valve manipulation. Rather, it involves verification that those valves outside containment and capable of potentially being mispositioned are in the correct position.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.6.7.2

To provide effective iodine removal, the containment spray must be an alkaline solution. Since the refueling water tank contents are normally acidic, the volume of the spray additive tank must provide a sufficient volume of spray additive to adjust pH for all water injected. This SR is performed to verify the availability of sufficient hydrazine (N_2H_4) solution in the Spray Additive System. The 184 day Frequency is based on the low probability of an undetected change in tank volume occurring during the SR interval (the tank is isolated during normal unit operations). Tank level is also indicated and alarmed in the control room, such that there is a high confidence that a substantial change in level would be detected.

SR 3.6.7.3

This SR provides verification of the N_2H_4 concentration in the spray additive tank and is sufficient to ensure that the spray solution being injected into containment is at the correct pH level. The concentration of N_2H_4 in the spray additive tank must be determined by chemical analysis. The 184 day Frequency is sufficient to ensure that the concentration level of N_2H_4 in the spray additive tank remains within the established limits. This is based on the low likelihood of an uncontrolled change in concentration (the tank is normally isolated) and the probability that any substantial variance in tank volume will be detected.

[SR 3.6.7.4

The chemical addition pump must be verified to provide the flow rate assumed in the accident analysis to the Containment Spray System. The Spray Additive System is not operated during normal operations. This prevents periodically subjecting systems, structures, and components within containment to a caustic spray solution. Therefore, this test must be performed on recirculation with the discharge flow path from each spray chemical addition pump aligned back to the spray additive tank. The differential pressure obtained by the pump on recirculation is analogous to the full spray additive flow provided to the Containment Spray System on an actual CSAS. The Frequency of this SR is in accordance with the Inservice Testing Program and is sufficient to identify component degradation that may affect flow rate.]

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.6.7.5

This SR verifies that each automatic valve in the Spray Additive System flow path actuates to its correct position on a CSAS. This Surveillance is not required for valves that are locked, sealed, or otherwise secured in the required position under administrative controls. The [18] month Frequency is based on the need to perform this Surveillance under the conditions that apply during a plant outage and the potential for an unplanned transient if the Surveillance were performed with the reactor at power. Operating experience has shown that these components usually pass the Surveillance when performed at the [18] month Frequency. Therefore, the Frequency was concluded to be acceptable from a reliability standpoint.

[SR 3.6.7.6

To ensure that the correct pH level is established in the borated water solution provided by the Containment Spray System, the flow rate in the Spray Additive System is verified once per 5 years. This SR provides assurance that the correct amount of N_2H_4 will be metered into the flow path upon Containment Spray System initiation. Due to the passive nature of the spray additive flow controls, the 5 year Frequency is sufficient to identify component degradation that may affect flow rate.]

REFERENCES

1. FSAR, Section [ ].

B 3.6 CONTAINMENT SYSTEMS

B 3.6.8 Shield Building Exhaust Air Cleanup System (SBEACS) (Dual)

BASES

BACKGROUND

The SBEACS is required by 10 CFR 50, Appendix A, GDC 41, "Containment Atmosphere Cleanup" (Ref. 1), to ensure that radioactive material leaking from the primary containment of a dual containment into the shield building (secondary containment) following a Design Basis Accident are filtered and adsorbed prior to exhausting to the environment.

The containment has a secondary containment, the shield building, which is a concrete structure that surrounds the steel primary containment vessel. Between the containment vessel and the shield building inner wall is an annular space that collects any containment leakage that may occur following a loss of coolant accident (LOCA). This space also allows for periodic inspection of the outer surface of the steel containment vessel.

Following a LOCA, the SBEACS establishes a negative pressure in the annulus between the shield building and the steel containment vessel. Filters in the system then control the release of radioactive contaminants to the environment. Shield building OPERABILITY is required to ensure retention of primary containment leakage and proper operation of the SBEACS.

The SBEACS consists of two separate and redundant trains. Each train includes a heater, cooling coils, a prefilter, a moisture separator, a high efficiency particulate air (HEPA) filter, an activated charcoal adsorber section for removal of radioiodines, and a fan. Ductwork, valves and/or dampers, and instrumentation also form part of the system. The moisture separators function to reduce the moisture content of the airstream. A second bank of HEPA filters follows the adsorber section to collect carbon fines and provide backup in case of failure of the main HEPA filter bank. Only the upstream HEPA filter and the charcoal adsorber section are credited in the analysis. The system initiates and maintains a negative air pressure in the shield building by means of filtered exhaust ventilation of the shield building following receipt of a safety injection actuation signal (SIAS). The system is described in Reference 2.

The prefilters remove any large particles in the air, and the moisture separators remove any entrained water droplets present, to prevent excessive loading of the HEPA filters and charcoal adsorbers. Heaters may be included to reduce the relative humidity of the airstream on

BASES

BACKGROUND (continued)

systems operating in high humidity. Continuous operation of each train for at least 10 hours per month with heaters on reduces moisture buildup on the HEPA filters and adsorbers. [The cooling coils cool the air to keep the charcoal beds from becoming too hot due to absorption of fission products.]

During normal operation, the Shield Building Cooling System is aligned to bypass the SBEACS HEPA filters and charcoal adsorbers. For SBEACS operation following a DBA, however, the bypass dampers automatically reposition to draw the air through the filters and adsorbers.

The SBEACS reduces the radioactive content in the shield building atmosphere following a DBA. Loss of the SBEACS could cause site boundary doses, in the event of a DBA, to exceed the values given in the licensing basis.

APPLICABLE SAFETY ANALYSES

The SBEACS design basis is established by the consequences of the limiting DBA, which is a LOCA. The accident analysis (Ref. 3) assumes that only one train of the SBEACS is functional due to a single failure that disables the other train. The accident analysis accounts for the reduction in airborne radioactive material provided by the remaining one train of this filtration system. The amount of fission products available for release from containment is determined for a LOCA.

The modeled SBEACS actuation in the safety analysis is based on a worst case response time associated with exceeding an SIAS. The total response time from exceeding the signal setpoint to attaining the negative pressure of [≥ 0.25] inch water gauge in the shield building is [1 minute]. This response time is composed of signal delay, diesel generator startup and sequencing time, system startup time, and time for the system to attain the required pressure after starting.

The SBEACS satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

In the event of a DBA, one SBEACS train is required to provide the minimum particulate iodine removal assumed in the safety analysis. Two trains of the SBEACS must be OPERABLE to ensure that at least one train will operate, assuming that the other train is disabled by a single active failure.

BASES

APPLICABILITY

In MODES 1, 2, 3, and 4, a DBA could lead to fission product release to containment that leaks to the shield building. The large break LOCA, on which this system's design is based, is a full power event. Less severe LOCAs and leakage still require the system to be OPERABLE throughout these MODES. The probability and severity of a LOCA decrease as core power and Reactor Coolant System pressure decrease. With the reactor shut down, the probability of release of radioactivity resulting from such an accident is low.

In MODES 5 and 6, the probability and consequences of a DBA are low due to the pressure and temperature limitations in these MODES. Under these conditions, the Filtration System is not required to be OPERABLE.

ACTIONS

A.1

With one SBEACS train inoperable, the inoperable train must be restored to OPERABLE status within 7 days. The components in this degraded condition are capable of providing 100% of the iodine removal needs after a DBA. The 7 day Completion Time is based on consideration of such factors as the availability of the OPERABLE redundant SBEACS train and the low probability of a DBA occurring during this period.

B.1 and B.2

If the SBEACS train cannot be restored to OPERABLE status within the required Completion Time, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 5 within 36 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.6.8.1

Operating each SBEACS train for ≥ 15 minutes ensures that all trains are OPERABLE and that all associated controls are functioning properly. It also ensures that blockage, fan or motor failure, or excessive vibration can be detected for corrective action. For systems with heaters, operation with the heaters on (automatic heater cycling to maintain temperature) for ≥ 10 continuous hours eliminates moisture on the adsorbers and HEPA filters. Experience from filter testing at operating units indicates that the 10 hour period is adequate for moisture

BASES

SURVEILLANCE REQUIREMENTS (continued)

elimination on the adsorbers and HEPA filters. The 31 day Frequency was developed considering the known reliability of fan motors and controls, the two train redundancy available, and the iodine removal capability of the Containment Spray System.

SR 3.6.8.2

This SR verifies that the required SBEACS filter testing is performed in accordance with the Ventilation Filter Testing Program (VFTP). The VFTP includes testing of HEPA filter performance, charcoal adsorber efficiency, minimum system flow rate, and the physical properties of the activated charcoal (general use and following specific operations). Specific test frequencies and additional information are discussed in detail in the VFTP.

SR 3.6.8.3

The automatic startup ensures that each SBEACS train responds properly. The [18] month Frequency is based on the need to perform this Surveillance under the conditions that apply during a plant outage and the potential for an unplanned transient if the Surveillance were performed with the reactor at power. Operating experience has shown that these components usually pass the Surveillance when performed at the [18] month Frequency. Therefore, the Frequency was concluded to be acceptable from a reliability standpoint. Furthermore, the SR interval was developed considering that the SBEACS equipment OPERABILITY is demonstrated at a 31 day Frequency by SR 3.6.8.1.

[SR 3.6.8.4

The filter bypass dampers are tested to verify OPERABILITY. The dampers are in the bypass position during normal operation and must reposition for accident operation to draw air through the filters. The [18] month Frequency is considered to be acceptable based on the damper reliability and design, the mild environmental conditions in the vicinity of the dampers, and the fact that operating experience has shown that the dampers usually pass the Surveillance when performed at the [18] month Frequency.]

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.6.8.5

The SBEACS train flow rate is verified ≥ [ ] cfm to ensure that the flow rate is adequate to "pull down" the shield building pressure as required. This test also will verify the proper functioning of the fans, dampers, filters, absorbers, etc., when this SR is performed in conjunction with SR 3.6.11.4.

The [18] month on a STAGGERED TEST BASIS Frequency is consistent with the Regulatory Guide 1.52 (Ref. 4) guidance.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 41.
2. FSAR, Section [ ].
3. FSAR, Section [ ].
4. Regulatory Guide 1.52, Revision [2].

B 3.6 CONTAINMENT SYSTEMS

B 3.6.9 Hydrogen Mixing System (HMS) (Atmospheric and Dual)

BASES

BACKGROUND

The HMS reduces the potential for breach of containment due to a hydrogen oxygen reaction by providing a uniformly mixed post accident containment atmosphere, thereby minimizing the potential for local hydrogen burns due to a local pocket of hydrogen above the flammable concentration and giving the operator the capability of preventing the occurrence of a bulk hydrogen burn inside containment per 10 CFR 50.44, "Standards for Combustible Gas Control Systems in Light-Water-Cooled Reactors" (Ref. 1), and 10 CFR 50, GDC 41, "Containment Atmosphere Cleanup" (Ref. 2).

The post accident HMS is an Engineered Safety Feature and is designed to withstand a loss of coolant accident (LOCA) without loss of function. The system has two independent trains, each of which consists of two dome air circulation fans, motors, and controls. Each train is sized for [37,000] cfm. The two trains are initiated automatically on a containment cooling actuation signal (CCAS) or can be manually started from the control room. Each train is powered from a separate emergency power supply. Since each train can provide 100% of the mixing requirements, the system will provide its design function with a limiting single active failure.

The HMS accelerates the air mixing process between the upper dome space of the containment atmosphere during LOCA operations. It also prevents any hot spot air pockets during the containment cooling mode and avoids any hydrogen concentration in pocket areas.

Hydrogen mixing within the containment is accomplished by the Containment Spray System, the containment emergency fan coolers, and the containment internal structure design, which permits convective mixing and prevents entrapment. The HMS, operating in conjunction with the Containment Spray System and the emergency fan coolers, prevents localized accumulations of hydrogen from exceeding the flammability limit of 4.1 volume percent (v/o).

APPLICABLE SAFETY ANALYSES

The HMS mixes the containment atmosphere to provide a uniform hydrogen concentration.

Hydrogen may accumulate in containment following a LOCA as a result of:

BASES

APPLICABLE SAFETY ANALYSES (continued)

a. A metal steam reaction between the zirconium fuel rod cladding and the reactor coolant,

b. Radiolytic decomposition of water in the Reactor Coolant System (RCS) and the containment sump,

c. Hydrogen in the RCS at the time of the LOCA (i.e., hydrogen dissolved in the reactor coolant and hydrogen gas in the pressurizer vapor space), or

d. Corrosion of metals exposed to Containment Spray System and Emergency Core Cooling Systems solutions.

To evaluate the potential for hydrogen accumulation in containment following a LOCA, the hydrogen generation as a function of time following the initiation of the accident is calculated. Conservative assumptions recommended by Reference 3 are used to maximize the amount of hydrogen calculated.

The HMS satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

Two HMS trains must be OPERABLE, with power to each from an independent, safety related power supply. Each train typically consists of two fans with their own motors and controls and is automatically initiated by a CCAS.

Operation with at least one HMS train provides the mixing necessary to ensure uniform hydrogen concentration throughout containment.

APPLICABILITY

In MODES 1 and 2, the two HMS trains ensure the capability to prevent localized hydrogen concentrations above the flammability limit of 4.1 v/o in containment, assuming a worst case single active failure.

In MODE 3 or 4, both the hydrogen production rate and the total hydrogen produced after a LOCA would be less than that calculated for the DBA LOCA. Also, because of the limited time in these MODES, the probability of an accident requiring the HMS is low. Therefore, the HMS is not required in MODE 3 or 4.

In MODES 5 and 6, the probability and consequences of a LOCA or main steam line break are low due to the pressure and temperature limitations of these MODES. Therefore, the HMS is not required in these MODES.

BASES

ACTIONS

A.1

With one HMS train inoperable, the inoperable train must be restored to OPERABLE status within 30 days. The 30 day Completion Time is based on the availability of the other HMS train, the small probability of a LOCA or SLB occurring (that would generate an amount of hydrogen that exceeds the flammability limit), the amount of time available after a LOCA or SLB (should one occur) for operator action to prevent hydrogen accumulation from exceeding the flammability limit, and the availability of the Containment Spray System and Hydrogen Purge System.

B.1 and B.2

-----------------------------------REVIEWER'S NOTE-----------------------------------
This Condition is only allowed for units with an alternate hydrogen control system acceptable to the technical staff.

With two HMS inoperable, the ability to perform the hydrogen control function via alternate capabilities must be verified by administrative means within 1 hour. The alternate hydrogen control capabilities are provided by [the containment Hydrogen Purge System/Hydrogen Ignitor System/HMS/Containment Air Dilution System/Containment Inerting System]. The 1 hour Completion Time allows a reasonable period of time to verify that a loss of hydrogen control function does not exist.

-----------------------------------REVIEWER'S NOTE-----------------------------------
The following is to be used if a non-Technical Specification alternate hydrogen control function is used to justify this Condition. In addition, the alternate hydrogen control system capability must be verified every 12 hours thereafter to ensure its continued availability.

[Both] the [initial] verification [and all subsequent verifications] may be performed as an administrative check, by examining logs or other information to determine the availability of the alternate hydrogen control system. It does not mean to perform the Surveillances needed to demonstrate OPERABILITY of the alternate hydrogen control system. If the ability to perform the hydrogen control function is maintained, continued operation is permitted with two HMS trains inoperable for up to 7 days. Seven days is a reasonable time to allow two HMS trains to be inoperable because the hydrogen control function is maintained and because of the low probability of the occurrence of a LOCA that would generate hydrogen in the amounts capable of exceeding the flammability limit.

BASES

ACTIONS (continued)

C.1

If an inoperable HMS train cannot be restored to OPERABLE status within the required Completion Time, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours. The allowed Completion Time of 6 hours is reasonable, based on operating experience, to reach MODE 3 from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.6.9.1

Operating each HMS train for ≥ 15 minutes ensures that the train is OPERABLE and that all associated controls are functioning properly. It also ensures that blockage, fan and/or motor failure, or excessive vibration can be detected for corrective action. The 92 day Frequency is consistent with Inservice Testing Program Surveillance Frequencies, operating experience, the known reliability of the fan motors and controls, and the two train redundancy available.

SR 3.6.9.2

Verifying that each HMS train flow rate on slow speed is ≥ [37,000] cfm ensures that each train is capable of maintaining localized hydrogen concentrations below the flammability limit. The [18] month Frequency is based on the need to perform this Surveillance under the conditions that apply during a plant outage and the potential for an unplanned transient if the Surveillance were performed with the reactor at power. Operating experience has shown that these components usually pass the Surveillance when performed at the [18] month Frequency. Therefore, the Frequency was concluded to be acceptable from a reliability standpoint.

SR 3.6.9.3

This SR ensures that the HMS responds properly to a CCAS. The [18] month Frequency is based on the need to perform this Surveillance under the conditions that apply during a plant outage and the potential for an unplanned transient if the Surveillance were performed with the reactor at power. Operating experience has shown that these components usually pass the Surveillance when performed at the [18] month Frequency. Therefore, the Frequency was concluded to be acceptable from a reliability standpoint.

BASES

REFERENCES

1. 10 CFR 50.44.

2. 10 CFR 50, Appendix A, GDC 41.

3. Regulatory Guide 1.7, Revision [1].

B 3.6 CONTAINMENT SYSTEMS

B 3.6.10 Iodine Cleanup System (ICS) (Atmospheric and Dual)

BASES

BACKGROUND

The ICS is provided per GDC 41, "Containment Atmosphere Cleanup," GDC 42, "Inspection of Containment Atmosphere Cleanup Systems," and GDC 43, "Testing of Containment Atmosphere Cleanup Systems" (Ref. 1), to reduce the concentration of fission products released to the containment atmosphere following a postulated accident. The ICS would function together with the Containment Spray and Cooling systems following a Design Basis Accident (DBA) to reduce the potential release of radioactive material, principally iodine, from the containment to the environment.

The ICS consists of two 100% capacity separate, independent, and redundant trains. Each train includes a heater, [cooling coils,] a prefilter, a moisture separator, a high efficiency particulate air (HEPA) filter, an activated charcoal adsorber section for removal of radioiodines, and a fan. Ductwork, valves and/or dampers, and instrumentation also form part of the system. The moisture separators function to reduce the moisture content of the airstream. A second bank of HEPA filters follows the adsorber section to collect carbon fines and provide backup in case of failure of the main HEPA filter bank. Only the upstream HEPA filter and the charcoal adsorber section are credited in the analysis. The system initiates filtered recirculation of the containment atmosphere following receipt of a containment isolation actuation signal. The system design is described in Reference 2.

The primary purpose of the heaters is to ensure that the relative humidity of the airstream entering the charcoal adsorbers is maintained below 70%, which is consistent with the assigned iodine and iodide removal efficiencies as per Regulatory Guide 1.52 (Ref. 3).

The moisture separator is included for moisture (free water) removal from the gas stream. Heaters are used to heat the gas stream, which lowers the relative humidity. Continuous operation of each train for at least 10 hours per month with the heaters on reduces moisture buildup on the HEPA filters and adsorbers. Both the moisture separator and heater are important to the effectiveness of the charcoal adsorbers.

Two ICS trains are provided to meet the requirement for separation, independence, and redundancy. Each ICS train is powered from a separate Engineered Safety Features bus and is provided with a separate power panel and control panel. [Service water is required to supply cooling water to the cooling coils.]

BASES

APPLICABLE SAFETY ANALYSES	The DBAs that result in a release of radioactive iodine within containment are a loss of coolant accident (LOCA), a main steam line break (MSLB), or a control element assembly (CEA) ejection accident. In the analysis for each of these accidents, it is assumed that adequate containment leak tightness is intact at event initiation to limit potential leakage to the environment. Additionally, it is assumed that the amount of radioactive iodine release is limited by reducing the iodine concentration in the containment atmosphere. The ICS design basis is established by the consequences of the limiting DBA, which is a LOCA. The accident analysis (Ref. 4) assumes that only one train of the ICS is functional due to a single failure that disables the other train. The accident analysis accounts for the reduction in airborne radioactive iodine provided by the remaining one train of this filtration system. The ICS satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).
LCO	Two separate, independent, and redundant trains of the ICS are required to ensure that at least one is available, assuming a single failure coincident with a loss of offsite power.
APPLICABILITY	In MODES 1, 2, 3, and 4, iodine is a fission product that can be released from the fuel to the reactor coolant as a result of a DBA. The DBAs that can cause a failure of the fuel cladding are a LOCA, MSLB, and CEA ejection accident. Because these accidents are considered credible accidents in MODES 1, 2, 3, and 4, the ICS must be operable in these MODES to ensure the reduction in iodine concentration assumed in the accident analysis. In MODES 5 and 6, the probability and consequences of a LOCA are low due to the pressure and temperature limitations of these MODES. The ICS is not required in these MODES to remove iodine from the containment atmosphere.
ACTIONS	<u>A.1</u> With one ICS train inoperable, the inoperable train must be restored to OPERABLE status within 7 days. The components in this degraded condition are capable of providing 100% of the iodine removal needs after a DBA. The 7 day Completion Time is based on consideration of such factors as: a. The availability of the OPERABLE redundant ICS train,

BASES

ACTIONS (continued)

b. The fact that, even with no ICS train in operation, almost the same amount of iodine would be removed from the containment atmosphere through absorption by the Containment Spray System, and

c. The fact that the Completion Time is adequate to make most repairs.

B.1 and B.2

If the ICS train cannot be restored to OPERABLE status within the required Completion Time, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 5 within 36 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.6.10.1

Operating each ICS train for ≥ 15 minutes ensures that all trains are OPERABLE and that all associated controls are functioning properly. It also ensures that blockage, fan or motor failure, or excessive vibration can be detected for corrective action. For systems with heaters, operation with the heaters on (automatic heater cycling to maintain temperature) for ≥ 10 continuous hours eliminates moisture on the adsorbers and HEPA filters. Experience from filter testing at operating units indicates that the 10 hour period is adequate for moisture elimination on the adsorbers and HEPA filters. The 31 day Frequency was developed considering the known reliability of fan motors and controls, the two train redundancy available, and the iodine removal capability of the Containment Spray System independent of the ICS.

SR 3.6.10.2

This SR verifies that the required ICS filter testing is performed in accordance with the Ventilation Filter Testing Program (VFTP). The VFTP includes testing HEPA filter performance, charcoal adsorber efficiency, minimum system flow rate, and the physical properties of the activated charcoal (general use and following specific operations). Specific test frequencies and additional information are discussed in detail in the VFTP.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.6.10.3

The automatic startup test verifies that both trains of equipment start upon receipt of an actual or simulated test signal. The [18] month Frequency is based on the need to perform this Surveillance under the conditions that apply during a plant outage and the potential for an unplanned transient if the Surveillance were performed with the reactor at power. Operating experience has shown that these components usually pass the Surveillance when performed at the [18] month Frequency. Therefore, the Frequency was concluded to be acceptable from a reliability standpoint. Furthermore, the Frequency was developed considering that the system equipment OPERABILITY is demonstrated on a 31 day Frequency by SR 3.6.10.1.

[SR 3.6.10.4

The ICS filter bypass dampers are tested to verify OPERABILITY. The dampers are in the bypass position during normal operation and must reposition for accident operation to draw air through the filters. The [18] month Frequency is considered to be acceptable based on the damper reliability and design, the mild environmental conditions in the vicinity of the dampers, and the fact that operating experience has shown that the dampers usually pass the Surveillance when performed at the [18] month Frequency.]

REFERENCES

1. 10 CFR 50, Appendix A, GDC 41, GDC 42, and GDC 43.
2. FSAR, Section [ ].
3. Regulatory Guide 1.52, Revision [2].
4. FSAR, Section [ ].

B 3.6 CONTAINMENT SYSTEMS

B 3.6.11 Shield Building (Dual)

BASES

BACKGROUND	The shield building is a concrete structure that surrounds the steel containment vessel. Between the containment vessel and the shield building inner wall is an annular space that collects any containment leakage that may occur following a loss of coolant accident (LOCA). This space also allows for periodic inspection of the outer surface of the steel containment vessel. Following a LOCA, the Shield Building Exhaust Air Cleanup System (SBEACS) establishes a negative pressure in the annulus between the shield building and the steel containment vessel. Filters in the system then control the release of radioactive contaminants to the environment. A description of the SBEACS is provided in the Bases for Specification 3.6.8, "Shield Building Exhaust Air Cleanup System (SBEACS)." Shield building OPERABILITY is required to ensure retention of primary containment leakage and proper operation of the SBEACS.
APPLICABLE SAFETY ANALYSES	The design basis for shield building OPERABILITY is a large break LOCA. Maintaining shield building OPERABILITY ensures that the release of radioactive material from the primary containment atmosphere is restricted to those leakage paths and associated leakage rates assumed in the accident analysis. The shield building satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).
LCO	Shield building OPERABILITY must be maintained to ensure proper operation of the SBEACS and to limit radioactive leakage from the containment to those paths and leakage rates assumed in the accident analysis.
APPLICABILITY	Maintaining shield building OPERABILITY prevents leakage of radioactive material from the shield building. Radioactive material may enter the shield building from the primary containment following a LOCA. Therefore, shield building OPERABILITY is required in MODES 1, 2, 3, and 4 when a main steam line break, LOCA, or control element assembly ejection accident could release radioactive material to the primary containment atmosphere. In MODES 5 and 6, the probability and consequences of these events are low due to the Reactor Coolant System temperature and pressure limitations in these MODES. Therefore, shield building OPERABILITY is not required in MODE 5 or 6.

BASES

ACTIONS

A.1

In the event shield building OPERABILITY is not maintained, shield building OPERABILITY must be restored within 24 hours.

Twenty-four hours is a reasonable Completion Time considering the limited leakage design of the containment and the low probability of a DBA occurring during this time period.

B.1 and B.2

If the shield building cannot be restored to OPERABLE status within the required Completion Time, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 5 within 36 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.6.11.1

Verifying that shield building annulus pressure is within limit ensures that operation remains within the limit assumed in the containment analysis. The 12 hour Frequency of this SR was developed considering operating experience related to shield building annulus pressure variations and pressure instrument drift during the applicable MODES.

SR 3.6.11.2

Maintaining shield building OPERABILITY requires verifying one door in the access opening closed. [An access opening may contain one inner and one outer door, or in some cases, shield building access openings are shared such that a shield building barrier may have multiple inner or multiple outer doors. The intent is to not breach the shield building boundary at any time when the shield building boundary is required. This is achieved by maintaining the inner or outer portion of the barrier closed at all times.] However, all shield building access doors are normally kept closed, except when the access opening is being used for entry and exit or when maintenance is being performed on an access opening. The Frequency of 31 days is based on engineering judgment and is considered adequate in view of other indications of door status available to the operator.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.6.11.3

This Surveillance would give advance indication of gross deterioration of the concrete structural integrity of the shield building. The Frequency of this SR is the same as that of SR 3.6.1.1. The verification is done during shutdown and as part of Type A leakage tests associated with SR 3.6.1.1.

SR 3.6.11.4

The SBEACS produces a negative pressure to prevent leakage from the building. SR 3.6.11.4 verifies that the shield building can be rapidly drawn down to ≥ [0.25] inch water. This test is used to ensure shield building boundary integrity. Establishment of this pressure is confirmed by SR 3.6.11.4, which demonstrates that the shield building can be drawn down to ≥ [0.25] inches of water ≤ 1 minute using one SBEACS train. The time limit ensures that no significant quantity of radioactive material leaks from the shield building prior to developing the negative pressure. Since this SR is a shield building boundary integrity test, it does not need to be performed with each SBEACS train. The SBEACS train used for this Surveillance is staggered to ensure that in addition to the requirements of LCO 3.6.11.4, either train will perform this test. The primary purpose of this SR is to ensure shield building integrity. The secondary purpose of this SR is to ensure that the SBEACS being tested functions as designed. The inoperability of the SBEACS train does not necessarily constitute a failure of this Surveillance relative to the shield building OPERABILITY. The 18 month Frequency is consistent with Regulatory Guide 1.52 (Ref. 1) guidance for functional testing of the ability of the SBEACS.

REFERENCES

1. Regulatory Guide 1.52, Revision [2].

B 3.6 CONTAINMENT SYSTEMS

B 3.6.12 Vacuum Relief Valves (Dual)

BASES

BACKGROUND

The vacuum relief valves protect the containment vessel against negative pressure (i.e., a lower pressure inside than outside). Excessive negative pressure inside containment can occur if there is an inadvertent actuation of the Containment Cooling System or the Containment Spray System. Multiple equipment failures or human errors are necessary to have inadvertent actuation.

The containment pressure vessel contains two 100% vacuum relief lines installed in parallel that protect the containment from excessive external loading. The vacuum relief lines are 24 inch penetrations that connect the shield building annulus to the containment. Each vacuum relief line is isolated by a pneumatically operated butterfly valve in series with a check valve located on the containment side of the penetration.

Each butterfly valve is actuated by a separate pressure controller that senses the differential pressure between the containment and the annulus. Each butterfly valve is provided with an air accumulator that allows the valve to open following a loss of instrument air.

The combined pressure drop at rated flow through either vacuum relief line will not exceed the containment pressure vessel design external pressure differential of [0.65] psig with any prevailing atmospheric pressure.

APPLICABLE SAFETY ANALYSES

Design of the vacuum relief lines involves calculating the effect of an inadvertent containment spray actuation that can reduce the atmospheric temperature (and hence pressure) inside containment (Ref. 1). Conservative assumptions are used for all the pertinent parameters in the calculation. For example, the minimum spray water temperature is assumed, as well as maximum initial containment temperature, maximum spray flow, all trains of spray operating, etc. The resulting containment pressure versus time is calculated, including the effect of the vacuum relief valves opening when their negative pressure setpoint is reached. It is also assumed that one vacuum relief line fails to open.

The containment was designed for an external pressure load equivalent to [0.65] psig. The inadvertent actuation of the Containment Spray System was analyzed to determine the resulting reduction in containment pressure. The initial pressure condition used in this analysis was [-0.368] psig. This resulted in a minimum pressure inside containment of [0.49] psig, which is less than the design load.

BASES

APPLICABLE SAFETY ANALYSES (continued)

The vacuum relief valves must also perform the containment isolation function in a containment high pressure event. For this reason, the system is designed to take the full containment positive design pressure and the containment design basis accident (DBA) environmental conditions (temperature, pressure, humidity, radiation, chemical attack, etc.) associated with the containment DBA.

The vacuum relief valves satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

The LCO establishes the minimum equipment required to accomplish the vacuum relief function following the inadvertent actuation of the Containment Spray System. Two vacuum relief lines are required to be OPERABLE to ensure that at least one is available, assuming one or both valves in the other line fail to open.

APPLICABILITY

In MODES 1, 2, 3, and 4, the containment cooling features, such as the Containment Spray System, are required to be OPERABLE to mitigate the effects of a DBA. Excessive negative pressure inside containment could occur whenever these systems are required to be OPERABLE due to inadvertent actuation of these systems. Therefore, the vacuum relief lines are required to be OPERABLE in MODES 1, 2, 3, and 4 to mitigate the effects of inadvertent actuation of the Containment Spray System or Containment Cooling System.

In MODES 5 and 6, the probability and consequences of a DBA are reduced due to the pressure and temperature limitations of these MODES. The Containment Spray System and Containment Cooling System are not required to be OPERABLE in MODES 5 and 6. Therefore, maintaining OPERABLE vacuum relief lines is not required in MODE 5 or 6.

ACTIONS

A.1

With one of the required vacuum relief lines inoperable, the inoperable line must be restored to OPERABLE status within 72 hours. The specified time period is consistent with other LCOs for the loss of one train of a system required to mitigate the consequences of a LOCA or other DBA.

BASES

ACTIONS (continued)

B.1 and B.2

If the vacuum relief line cannot be restored to OPERABLE status within the required Completion Time, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 5 within 36 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.6.12.1

This SR references the Inservice Testing Program, which establishes the requirement that inservice testing of the ASME Code Class 1, 2, and 3 pumps and valves shall be performed in accordance with the ASME Boiler and Pressure Vessel Code and applicable Addenda (Ref. 2). Therefore, SR Frequency is governed by the Inservice Testing Program.

REFERENCES

1. FSAR, Section [6.2].

2. ASME Code for Operation and Maintenance of Nuclear Power Plants.

B 3.7 PLANT SYSTEMS

B 3.7.1 Main Steam Safety Valves (MSSVs)

BASES

BACKGROUND

The primary purpose of the MSSVs is to provide overpressure protection for the secondary system. The MSSVs also provide protection against overpressurizing the reactor coolant pressure boundary (RCPB) by providing a heat sink for the removal of energy from the Reactor Coolant System (RCS) if the preferred heat sink, provided by the Condenser and Circulating Water System, is not available.

Eight MSSVs are located on each main steam header, outside containment, upstream of the main steam isolation valves, as described in the FSAR, Section [5.2] (Ref. 1). The MSSV rated capacity passes the full steam flow at 102% RTP (100% + 2% for instrument error) with the valves full open. This meets the requirements of the ASME Code, Section III (Ref. 2). The MSSV design includes staggered setpoints, according to Table 3.7.1-1, in the accompanying LCO, so that only the number of valves needed will actuate. Staggered setpoints reduce the potential for valve chattering because of insufficient steam pressure to fully open all valves following a turbine reactor trip.

APPLICABLE SAFETY ANALYSES

The design basis for the MSSVs comes from Reference 2. The MSSV's purpose is to limit secondary system pressure to ≤ 110% of design pressure when passing 100% of design steam flow. This design basis is sufficient to cope with any anticipated operational occurrence (AOO) or accident considered in the Design Basis Accident (DBA) and transient analysis.

The events that challenge the MSSV relieving capacity, and thus RCS pressure, are those characterized as decreased heat removal events, and are presented in the FSAR, Section [15.2] (Ref. 3). Of these, the full power loss of condenser vacuum (LOCV) event is the limiting AOO. An LOCV isolates the turbine and condenser, and terminates normal feedwater flow to the steam generators. Before delivery of auxiliary feedwater to the steam generators, RCS pressure reaches ≤ 2630 psig. This peak pressure is < 110% of the design pressure of 2500 psig, but high enough to actuate the pressurizer safety valves. The maximum relieving rate during the LOCV event is 2.5 E6 lb/hour, which is less than the rated capacity of two MSSVs.

BASES

APPLICABLE SAFETY ANALYSES (continued)

The limiting accident for peak RCS pressure is the full power feedwater line break (FWLB), inside containment, with the failure of the backflow check valve in the feedwater line from the affected steam generator. Water from the affected steam generator is assumed to be lost through the break with minimal additional heat transfer from the RCS. With heat removal limited to the unaffected steam generator, the reduced heat transfer causes an increase in RCS temperature, and the resulting RCS fluid expansion causes an increase in pressure. The RCS pressure increases to ≤ 2730 psig, with the pressurizer safety valves providing relief capacity. The maximum relieving rate of the MSSVs during the FWLB event is ≤ 2.5 E6 lb/hour, which is less than the rated capacity of two MSSVs.

Using conservative analysis assumptions, a small range of FWLB sizes less than a full double ended guillotine break produce an RCS pressure of 2765 psig for a period of 20 seconds; exceeding 110% (2750 psig) of design pressure. This is considered acceptable as RCS pressure is still well below 120% of design pressure where deformation may occur. The probability of this event is in the range of 4 E-6/year.

The MSSVs satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

This LCO requires all MSSVs to be OPERABLE in compliance with Reference 2, even though this is not a requirement of the DBA analysis. This is because operation with less than the full number of MSSVs requires limitations on allowable THERMAL POWER (to meet Reference 2 requirements), and adjustment to the Reactor Protection System trip setpoints. These limitations are according to those shown in Table 3.7.1-1, Required Action A.1, and Required Action A.2 in the accompanying LCO. An MSSV is considered inoperable if it fails to open upon demand.

The OPERABILITY of the MSSVs is defined as the ability to open within the setpoint tolerances, relieve steam generator overpressure, and reseat when pressure has been reduced. The OPERABILITY of the MSSVs is determined by periodic surveillance testing in accordance with the Inservice Testing Program.

The lift settings, according to Table 3.7.1-2 in the accompanying LCO, correspond to ambient conditions of the valve at nominal operating temperature and pressure.

This LCO provides assurance that the MSSVs will perform their designed safety function to mitigate the consequences of accidents that could result in a challenge to the RCPB.

BASES

APPLICABILITY

In MODE 1, a minimum of two MSSVs per steam generator are required to be OPERABLE, according to Table 3.7.1-1 in the accompanying LCO, which is limiting and bounds all lower MODES. In MODES 2 and 3, both the ASME Code and the accident analysis require only one MSSV per steam generator to provide overpressure protection.

In MODES 4 and 5, there are no credible transients requiring the MSSVs.

The steam generators are not normally used for heat removal in MODES 5 and 6, and thus cannot be overpressurized; there is no requirement for the MSSVs to be OPERABLE in these MODES.

ACTIONS

The ACTIONS Table is modified by a Note indicating that separate Condition entry is allowed for each MSSV.

A.1 and A.2

An alternative to restoring the inoperable MSSV(s) to OPERABLE status is to reduce power so that the available MSSV relieving capacity meets Code requirements for the power level. Operation may continue provided the allowable THERMAL POWER is equal to the product of: 1) the ratio of the number of MSSVs available per steam generator to the total number of MSSVs per steam generator, and 2) the ratio of the available relieving capacity to total steam flow, multiplied by 100%.

$$\text{Allowable THERMAL POWER} = \left(\frac{8 - N}{8}\right) \times 109.2$$

With one or more MSSVs inoperable, the ceiling on the variable overpower trip is reduced to an amount over the allowable THERMAL POWER equal to the band given for this trip, according to Table 3.7.1-1 in the accompanying LCO.

SP = Allowable THERMAL POWER + 9.8

where:

SP = Reduced reactor trip setpoint in percent RTP. This is a ratio of the available relieving capacity over the total steam flow at rated power.

8 = Total number of MSSVs per steam generator.

N = Number of inoperable MSSVs on the steam generator with the greatest number of inoperable valves.

BASES

ACTIONS (continued)

109.2	=	Ratio of MSSV relieving capacity at 110% steam generator design pressure to calculated steam flow rate at 100% RTP + 2% instrument uncertainty expressed as a percentage (see text above).
9.8	=	Band between the maximum THERMAL POWER and the variable overpower trip setpoint ceiling (Table 3.7.1-1).

The operator should limit the maximum steady state power level to some value slightly below this setpoint to avoid an inadvertent overpower trip.

The 4 hour Completion Time for Required Action A.1 is a reasonable time period to reduce power level and is based on the low probability of an event occurring during this period that would require activation of the MSSVs. An additional 32 hours is allowed in Required Action A.2 to reduce the setpoints. The Completion Time of 36 hours for Required Action A.2 is based on a reasonable time to correct the MSSV inoperability, the time required to perform the power reduction, operating experience in resetting all channels of a protective function, and on the low probability of the occurrence of a transient that could result in steam generator overpressure during this period.

B.1 and B.2

If the MSSVs cannot be restored to OPERABLE status in the associated Completion Time, or if one or more steam generators have less than two MSSVs OPERABLE, the unit must be placed in a MODE in which the LCO does not apply. To achieve this status, the unit must be placed in at least MODE 3 within 6 hours, and in MODE 4 within [12] hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required unit conditions from full power conditions in an orderly manner and without challenging unit systems.

SURVEILLANCE REQUIREMENTS

SR 3.7.1.1

This SR verifies the OPERABILITY of the MSSVs by the verification of each MSSV lift setpoints in accordance with the Inservice Testing Program. The ASME Code (Ref. 4), requires that safety and relief valve tests be performed in accordance with ANSI/ASME OM-1-1987 (Ref. 5). According to Reference 5, the following tests are required for MSSVs:

BASES

SURVEILLANCE REQUIREMENTS (continued)

a. Visual examination,

b. Seat tightness determination,

c. Setpoint pressure determination (lift setting),

d. Compliance with owner's seat tightness criteria, and

e. Verification of the balancing device integrity on balanced valves.

The ANSI/ASME Standard requires that all valves be tested every 5 years, and a minimum of 20% of the valves be tested every 24 months. The ASME Code specifies the activities and frequencies necessary to satisfy the requirements. Table 3.7.1-2 allows a ± [3]% setpoint tolerance for OPERABILITY; however, the valves are reset to ± 1% during the Surveillance to allow for drift.

This SR is modified by a Note that allows entry into and operation in MODE 3 prior to performing the SR. This is to allow testing of the MSSVs at hot conditions. The MSSVs may be either bench tested or tested in situ at hot conditions using an assist device to simulate lift pressure. If the MSSVs are not tested at hot conditions, the lift setting pressure shall be corrected to ambient conditions of the valve at operating temperature and pressure.

REFERENCES

1. FSAR, Section [5.2].

2. ASME, Boiler and Pressure Vessel Code, Section III, Article NC-7000, Class 2 Components.

3. FSAR, Section [15.2].

4. ASME Code for Operation and Maintenance of Nuclear Power Plants.

5. ANSI/ASME OM-1-1987.

B 3.7 PLANT SYSTEMS

B 3.7.2 Main Steam Isolation Valves (MSIVs)

BASES

BACKGROUND

The MSIVs isolate steam flow from the secondary side of the steam generators following a high energy line break (HELB). MSIV closure terminates flow from the unaffected (intact) steam generator.

One MSIV is located in each main steam line outside, but close to, containment. The MSIVs are downstream from the main steam safety valves (MSSVs), atmospheric dump valves, and auxiliary feedwater pump turbine steam supplies to prevent their being isolated from the steam generators by MSIV closure. Closing the MSIVs isolates each steam generator from the other, and isolates the turbine, Steam Bypass System, and other auxiliary steam supplies from the steam generators.

The MSIVs close on a main steam isolation signal generated by either low steam generator pressure or high containment pressure. The MSIVs fail closed on loss of control or actuation power. The MSIS also actuates the main feedwater isolation valves (MFIVs) to close. The MSIVs may also be actuated manually.

A description of the MSIVs is found in the FSAR, Section [10.3] (Ref. 1).

APPLICABLE SAFETY ANALYSES

The design basis of the MSIVs is established by the containment analysis for the large steam line break (SLB) inside containment, as discussed in the FSAR, Section [6.2] (Ref. 2). It is also influenced by the accident analysis of the SLB events presented in the FSAR, Section [15.1.5] (Ref. 3). The design precludes the blowdown of more than one steam generator, assuming a single active component failure (e.g., the failure of one MSIV to close on demand).

The limiting case for the containment analysis is the hot zero power SLB inside containment with a loss of offsite power following turbine trip, and failure of the MSIV on the affected steam generator to close. At zero power, the steam generator inventory and temperature are at their maximum, maximizing the analyzed mass and energy release to the containment. Due to reverse flow, failure of the MSIV to close contributes to the total release of the additional mass and energy in the steam headers, which are downstream of the other MSIV. With the most reactive rod cluster control assembly assumed stuck in the fully

BASES

APPLICABLE SAFETY ANALYSES (continued)

withdrawn position, there is an increased possibility that the core will become critical and return to power. The core is ultimately shut down by the borated water injection delivered by the Emergency Core Cooling System. Other failures considered are the failure of an MFIV to close, and failure of an emergency diesel generator to start.

The accident analysis compares several different SLB events against different acceptance criteria. The large SLB outside containment upstream of the MSIV is limiting for offsite dose, although a break in this short section of main steam header has a very low probability. The large SLB inside containment at hot zero power is the limiting case for a post trip return to power. The analysis includes scenarios with offsite power available and with a loss of offsite power following turbine trip.

With offsite power available, the reactor coolant pumps continue to circulate coolant through the steam generators, maximizing the Reactor Coolant System (RCS) cooldown. With a loss of offsite power, the response of mitigating systems, such as the high pressure safety injection (HPSI) pumps, is delayed. Significant single failures considered include: failure of a MSIV to close, failure of an emergency diesel generator, and failure of a HPSI pump.

The MSIVs serve only a safety function and remain open during power operation. These valves operate under the following situations:

a. An HELB inside containment. In order to maximize the mass and energy release into the containment, the analysis assumes that the MSIV in the affected steam generator remains open. For this accident scenario, steam is discharged into containment from both steam generators until closure of the MSIV in the intact steam generator occurs. After MSIV closure, steam is discharged into containment only from the affected steam generator, and from the residual steam in the main steam header downstream of the closed MSIV in the intact loop.

b. A break outside of containment and upstream from the MSIVs. This scenario is not a containment pressurization concern. The uncontrolled blowdown of more than one steam generator must be prevented to limit the potential for uncontrolled RCS cooldown and positive reactivity addition. Closure of the MSIVs isolates the break, and limits the blowdown to a single steam generator.

BASES

APPLICABLE SAFETY ANALYSES (continued)

c. A break downstream of the MSIVs. This type of break will be isolated by the closure of the MSIVs. Events such as increased steam flow through the turbine or the steam bypass valves will also terminate on closure of the MSIVs.

d. A steam generator tube rupture. For this scenario, closure of the MSIV[s] isolates the affected steam generator from the intact steam generator. In addition to minimizing radiological releases, this enables the operator to maintain the pressure of the steam generator with the ruptured tube below the MSSV setpoints, a necessary step toward isolating the flow through the rupture.

e. The MSIVs are also utilized during other events such as a feedwater line break. These events are less limiting so far as MSIV OPERABILITY is concerned.

The MSIVs satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

This LCO requires that the MSIV in each of the [two] steam lines be OPERABLE. The MSIVs are considered OPERABLE when the isolation times are within limits, and they close on an isolation actuation signal.

This LCO provides assurance that the MSIVs will perform their design safety function to mitigate the consequences of accidents that could result in offsite exposures comparable to the 10 CFR 100 (Ref. 4) limits or the NRC staff approved licensing basis.

APPLICABILITY

The MSIVs must be OPERABLE in MODE 1 and in MODES 2 and 3 except when all MSIVs are closed and [deactivated]. In these MODES there is significant mass and energy in the RCS and steam generators. When the MSIVs are closed, they are already performing their safety function.

In MODE 4, the steam generator energy is low; therefore, the MSIVs are not required to be OPERABLE.

In MODES 5 and 6, the steam generators do not contain much energy because their temperature is below the boiling point of water; therefore, the MSIVs are not required for isolation of potential high energy secondary system pipe breaks in these MODES.

BASES

ACTIONS

A.1

With one MSIV inoperable in MODE 1, time is allowed to restore the component to OPERABLE status. Some repairs can be made to the MSIV with the unit hot. The [8] hour Completion Time is reasonable, considering the probability of an accident occurring during the time period that would require closure of the MSIVs.

The [8] hour Completion Time is greater than that normally allowed for containment isolation valves because the MSIVs are valves that isolate a closed system penetrating containment. These valves differ from other containment isolation valves in that the closed system provides an additional means for containment isolation.

B.1

If the MSIV cannot be restored to OPERABLE status within [8] hours, the unit must be placed in a MODE in which the LCO does not apply. To achieve this status, the unit must be placed in MODE 2 within 6 hours and Condition C would be entered. The Completion Time is reasonable, based on operating experience, to reach MODE 2, and close the MSIVs in an orderly manner and without challenging unit systems.

C.1, C.2.1, and C.2.2

Condition C is modified by a Note indicating that separate Condition entry is allowed for each MSIV.

Since the MSIVs are required to be OPERABLE in MODES 2 and 3, the inoperable MSIVs may either be restored to OPERABLE status or closed. When closed, the MSIVs are already in the position required by the assumptions in the safety analysis.

The [8] hour Completion Time is consistent with that allowed in Condition A.

Inoperable MSIVs that cannot be restored to OPERABLE status within the specified Completion Time, but are closed, must be verified on a periodic basis to be closed. This is necessary to ensure that the assumptions in the safety analysis remain valid. The 7 day Completion Time is reasonable, based on engineering judgment, MSIV status indications available in the control room, and other administrative controls, to ensure these valves are in the closed position.

BASES

ACTIONS (continued)

D.1 and D.2

If the MSIVs cannot be restored to OPERABLE status, or closed, within the associated Completion Time, the unit must be placed in a MODE in which the LCO does not apply. To achieve this status, the unit must be placed in at least MODE 3 within 6 hours, and in MODE 4 within [12] hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required unit conditions from MODE 2 conditions in an orderly manner and without challenging unit systems.

SURVEILLANCE REQUIREMENTS

SR 3.7.2.1

This SR verifies that the closure time of each MSIV is ≤ [4.6] seconds. The MSIV isolation time is assumed in the accident and containment analyses. This SR is normally performed upon returning the unit to operation following a refueling outage. The MSIVs should not be tested at power since even a part stroke exercise increases the risk of a valve closure with the unit generating power. As the MSIVs are not tested at power, they are exempt from the ASME Code (Ref. 5), requirements during operation in MODES 1 and 2.

The Frequency for this SR is in accordance with the Inservice Testing Program.

This test is conducted in MODE 3, with the unit at operating temperature and pressure. This SR is modified by a Note that allows entry into and operation in MODE 3 prior to performing the SR. This allows a delay of testing until MODE 3, in order to establish conditions consistent with those under which the acceptance criterion was generated.

SR 3.7.2.2

This SR verifies that each MSIV can close on an actual or simulated actuation signal. This Surveillance is normally performed upon returning the plant to operation following a refueling outage. The Frequency of MSIV testing is every [18] months. The [18] month Frequency for testing is based on the refueling cycle. Operating experience has shown that these components usually pass the Surveillance when performed at the [18] month Frequency. Therefore, this Frequency is acceptable from a reliability standpoint.

BASES

REFERENCES

1. FSAR, Section [10.3].
2. FSAR, Section [6.2].
3. FSAR, Section [15.1.5].
4. 10 CFR 100.11.
5. ASME Code for Operation and Maintenance of Nuclear Power Plants.

B 3.7 PLANT SYSTEMS

B 3.7.3 Main Feedwater Isolation Valves (MFIVs) [and [MFIV] Bypass Valves]

BASES

BACKGROUND

The MFIVs isolate main feedwater (MFW) flow to the secondary side of the steam generators following a high energy line break (HELB). Closure of the MFIVs and the bypass valves terminates flow to both steam generators, terminating the event for feedwater line breaks (FWLBs) occurring upstream of the MFIVs. The consequences of events occurring in the main steam lines or in the MFW lines downstream of the MFIVs will be mitigated by their closure. Closure of the MFIVs and bypass valves effectively terminates the addition of feedwater to an affected steam generator, limiting the mass and energy release for steam line breaks (SLBs) or FWLBs inside containment, and reducing the cooldown effects for SLBs.

The MFIVs and bypass valves isolate the nonsafety related portions from the safety related portion of the system. In the event of a secondary side pipe rupture inside containment, the valves limit the quantity of high energy fluid that enters containment through the break, and provide a pressure boundary for the controlled addition of auxiliary feedwater (AFW) to the intact loop.

One MFIV is located on each AFW line, outside, but close to, containment. The MFIVs are located upstream of the AFW injection point so that AFW may be supplied to a steam generator following MFIV closure. The piping volume from the valve to the steam generator must be accounted for in calculating mass and energy releases, and refilled prior to AFW reaching the steam generator following either an SLB or FWLB.

The MFIVs and its bypass valves close on receipt of a main steam isolation signal (MSIS) generated by either low steam generator pressure or high containment pressure. The MSIS also actuates the main steam isolation valves (MSIVs) to close. The MFIVs and bypass valves may also be actuated manually. In addition to the MFIVs and the bypass valves, a check valve inside containment is available to isolate the feedwater line penetrating containment, and to ensure that the consequences of events do not exceed the capacity of the containment heat removal systems.

A description of the MFIVs is found in the FSAR, Section [10.4.7] (Ref. 1).

BASES

APPLICABLE SAFETY ANALYSES	The design basis of the MFIVs is established by the analysis for the large SLB. It is also influenced by the accident analysis for the large FWLB. Closure of the MFIVs and their bypass valves may also be relied on to terminate a steam break for core response analysis and an excess feedwater flow event upon receipt of a MSIS on high steam generator level. Failure of an MFIV and the bypass valve to close following an SLB, FWLB, or excess feedwater flow event can result in additional mass and energy to the steam generators contributing to cooldown. This failure also results in additional mass and energy releases following an SLB or FWLB event. The MFIVs satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).
LCO	This LCO ensures that the MFIVs and the bypass valves will isolate MFW flow to the steam generators. Following an FWLB or SLB, these valves will also isolate the nonsafety related portions from the safety related portions of the system. This LCO requires that [two] MFIVs [and [MFIV] bypass valves] in each feedwater line be OPERABLE. The MFIVs and the bypass valves are considered OPERABLE when the isolation times are within limits, and are closed on an isolation actuation signal. Failure to meet the LCO requirements can result in additional mass and energy being released to containment following an SLB or FWLB inside containment. If an MSIS on high steam generator level is relied on to terminate an excess feedwater flow event, failure to meet the LCO may result in the introduction of water into the main steam lines.
APPLICABILITY	The MFIVs and the bypass valves must be OPERABLE whenever there is significant mass and energy in the Reactor Coolant System and steam generators. This ensures that, in the event of an HELB, a single failure cannot result in the blowdown of more than one steam generator. In MODES 1, 2, and 3, the MFIV [or [MFIV] bypass valves] are required to be OPERABLE, except when they are closed and deactivated or isolated by a closed manual valve, in order to limit the amount of available fluid that could be added to containment in the case of a secondary system pipe break inside containment. When the valves are closed and deactivated or isolated by a closed manual valve, they are already performing their safety function. In MODES 4, 5, and 6, steam generator energy is low. Therefore, the MFIVs and the bypass valves are normally closed since MFW is not required.

BASES

ACTIONS

The ACTIONS Table is modified by a Note indicating that separate Condition entry is allowed for each value.

A.1 and A.2

With one MFIV or the bypass valve inoperable, action must be taken to close or isolate the inoperable valves within [8 or 72] hours. When these valves are closed or isolated, they are performing their required safety function (e.g., to isolate the line).

For units with only one MFIV per feedwater line: The [8] hour Completion Time is reasonable to close the MFIV or its bypass valve, which includes performing a controlled unit shutdown to MODE 2.

The [72] hour Completion Time takes into account the redundancy afforded by the remaining OPERABLE valves, and the low probability of an event occurring during this time period that would require isolation of the MFW flow paths.

B.1

If more than one MFIV or [MFIV] bypass valve in the same flow path cannot be restored to OPERABLE status, then there may be no redundant system to operate automatically and perform the required safety function. Although the containment can be isolated with the failure of two valves in parallel in the same flow path, the double failure can be an indication of a common mode failure in the valves of this flow path, and as such is treated the same as a loss of the isolation capability of this flow path. Under these conditions, valves in each flow path must be restored to OPERABLE status, closed, or the flow path isolated within 8 hours. This action returns the system to the condition where at least one valve in each flow path is performing the required safety function. The 8 hour Completion Time is reasonable to close the MFIV or its bypass valve, or otherwise isolate the affected flow path.

Inoperable MFIVs and [MFIV] bypass valves that cannot be restored to OPERABLE status within the Completion Time, but are closed or isolated, must be verified on a periodic basis that they are closed or isolated. This is necessary to ensure that the assumptions in the safety analysis remain valid. The 7 day Completion Time is reasonable, based on engineering judgment, in view of valve status indications available in the control room, and other administrative controls to ensure that these valves are closed or isolated.

BASES

ACTIONS (continued)

C.1 and [C.2]

If the MFIVs and their bypass valves cannot be restored to OPERABLE status, closed, or isolated in the associated Completion Time, the unit must be placed in a MODE in which the LCO does not apply. To achieve this status, the unit must be placed in at least MODE 3 within 6 hours [, and in MODE 4 within [12] hours]. The allowed Completion Times are reasonable, based on operating experience, to reach the required unit conditions from full power conditions in an orderly manner and without challenging unit systems.

SURVEILLANCE REQUIREMENTS

SR 3.7.3.1

This SR ensures the verification of each MFIV [and [MFIV] bypass valve] is ≤ [7] seconds. The MFIV isolation time is assumed in the accident and containment analyses. This Surveillance is normally performed upon returning the unit to operation following a refueling outage. The MFIVs should not be tested at power since even a part stroke exercise increases the risk of a valve closure with the unit generating power. As these valves are not tested at power, they are exempt from the ASME Code (Ref. 2) requirements during operation in MODES 1 and 2.

The Frequency is in accordance with the Inservice Testing Program.

SR 3.7.3.2

This SR verifies that each MFIV [and [MFIV] bypass valve] can close on an actual or simulated actuation signal. This Surveillance is normally performed upon returning the plant to operation following a refueling outage.

The Frequency for this SR is every [18] months. The [18] month Frequency for testing is based on the refueling cycle. Operating experience has shown that these components usually pass the Surveillance when performed at the [18] month Frequency. Therefore, this Frequency is acceptable from a reliability standpoint.

REFERENCES

1. FSAR, Section [10.4.7].

2. ASME Code for Operation and Maintenance of Nuclear Power Plants.

B 3.7 PLANT SYSTEMS

B 3.7.4 Atmospheric Dump Valves (ADVs)

BASES

BACKGROUND

The ADVs provide a safety grade method for cooling the unit to Shutdown Cooling (SDC) System entry conditions, should the preferred heat sink via the Steam Bypass System to the condenser not be available, as discussed in the FSAR, Section [10.3] (Ref. 1). This is done in conjunction with the Auxiliary Feedwater System providing cooling water from the condensate storage tank (CST). The ADVs may also be required to meet the design cooldown rate during a normal cooldown when steam pressure drops too low for maintenance of a vacuum in the condenser to permit use of the Steam Bypass System.

Four ADV lines are provided. Each ADV line consists of one ADV and an associated block valve. Two ADV lines per steam generator are required to meet single failure assumptions following an event rendering one steam generator unavailable for Reactor Coolant System (RCS) heat removal.

The ADVs are provided with upstream block valves to permit their being tested at power, and to provide an alternate means of isolation. The ADVs are equipped with pneumatic controllers to permit control of the cooldown rate.

The ADVs are usually provided with a pressurized gas supply of bottled nitrogen that, on a loss of pressure in the normal instrument air supply, automatically supplies nitrogen to operate the ADVs. The nitrogen supply is sized to provide sufficient pressurized gas to operate the ADVs for the time required for RCS cooldown to the SDC System entry conditions.

A description of the ADVs is found in Reference 1. The ADVs are OPERABLE with only a DC power source available. In addition, hand wheels are provided for local manual operation.

APPLICABLE SAFETY ANALYSES

The design basis of the ADVs is established by the capability to cool the unit to SDC System entry conditions. A cooldown rate of 75°F per hour is obtainable by one or both steam generators. This design is adequate to cool the unit to SDC System entry conditions with only one ADV and one steam generator, utilizing the cooling water supply available in the CST.

BASES

APPLICABLE SAFETY ANALYSES (continued)

In the accident analysis presented in the FSAR, the ADVs are assumed to be used by the operator to cool down the unit to SDC System entry conditions for accidents accompanied by a loss of offsite power. Prior to the operator action, the main steam safety valves (MSSVs) are used to maintain steam generator pressure and temperature at the MSSV setpoint. This is typically 30 minutes following the initiation of an event. (This may be less for a steam generator tube rupture (SGTR) event.) The limiting events are those that render one steam generator unavailable for RCS heat removal, with a coincident loss of offsite power; this results from a turbine trip and the single failure of one ADV on the unaffected steam generator. Typical initiating events falling into this category are a main steam line break upstream of the main steam isolation valves, a feedwater line break, and an SGTR event (although the ADVs on the affected steam generator may still be available following a SGTR event).

The design must accommodate the single failure of one ADV to open on demand; thus, each steam generator must have at least two ADVs. The ADVs are equipped with block valves in the event an ADV spuriously opens, or fails to close during use.

The ADVs satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

[Two] ADV lines are required to be OPERABLE on each steam generator to ensure that at least one ADV is OPERABLE to conduct a unit cooldown following an event in which one steam generator becomes unavailable, accompanied by a single active failure of one ADV line on the unaffected steam generator. The block valves must be OPERABLE to isolate a failed open ADV. A closed block valve does not render it or its ADV line inoperable if operator action time to open the block valve is supported in the accident analysis.

Failure to meet the LCO can result in the inability to cool the unit to SDC System entry conditions following an event in which the condenser is unavailable for use with the Steam Bypass System.

An ADV is considered OPERABLE when it is capable of providing a controlled relief of the main steam flow, and is capable of fully opening and closing on demand.

BASES

APPLICABILITY

In MODES 1, 2, and 3, [and in MODE 4, when steam generator is being relied upon for heat removal,] the ADVs are required to be OPERABLE.

In MODES 5 and 6, an SGTR is not a credible event.

ACTIONS

A.1

With one required ADV line inoperable, action must be taken to restore the OPERABLE status within 7 days. The 7 day Completion Time takes into account the redundant capability afforded by the remaining OPERABLE ADV lines, and a nonsafety grade backup in the Steam Bypass System and MSSVs.

B.1

With [two] or more [required] ADV lines inoperable, action must be taken to restore [one] of the ADV lines to OPERABLE status. As the block valve can be closed to isolate an ADV, some repairs may be possible with the unit at power. The 24 hour Completion Time is reasonable to repair inoperable ADV lines, based on the availability of the Steam Bypass System and MSSVs, and the low probability of an event occurring during this period that requires the ADV lines.

C.1 and C.2

If the ADV lines cannot be restored to OPERABLE status within the associated Completion Time, the unit must be placed in a MODE in which the LCO does not apply. To achieve this status, the unit must be placed in at least MODE 3 within 6 hours, and in MODE 4, without reliance upon the steam generator for heat removal, within [24] hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required unit conditions from full power conditions in an orderly manner and without challenging unit systems.

SURVEILLANCE REQUIREMENTS

SR 3.7.4.1

To perform a controlled cooldown of the RCS, the ADVs must be able to be opened and throttled through their full range. This SR ensures the ADVs are tested through a full control cycle at least once per fuel cycle. Performance of inservice testing or use of an ADV during a unit cooldown may satisfy this requirement. Operating experience has shown that these components usually pass the SR when performed at the [18] month Frequency. Therefore, the Frequency is acceptable from a reliability standpoint.

BASES

SURVEILLANCE REQUIREMENTS (continued)

[SR 3.7.4.2

The function of the ADV block valve is to isolate a failed open ADV. Cycling the block valve closed and open demonstrates its capability to perform this function. Performance of inservice testing or use of the block valve during unit cooldown may satisfy this requirement. Operating experience has shown that these components usually pass the SR when performed at the [18] month Frequency. Therefore, the Frequency is acceptable from a reliability standpoint.]

REFERENCES

1. FSAR, Section [10.3].

B 3.7 PLANT SYSTEMS

B 3.7.5 Auxiliary Feedwater (AFW) System

BASES

BACKGROUND

The AFW System automatically supplies feedwater to the steam generators to remove decay heat from the Reactor Coolant System upon the loss of normal feedwater supply. The AFW pumps take suction through separate and independent suction lines from the condensate storage tank (CST) (LCO 3.7.6, "Condensate Storage Tank (CST)") and pump to the steam generator secondary side via separate and independent connections to the main feedwater (MFW) piping outside containment. The steam generators function as a heat sink for core decay heat. The heat load is dissipated by releasing steam to the atmosphere from the steam generators via the main steam safety valves (MSSVs) (LCO 3.7.1, "Main Steam Safety Valves (MSSVs)") or atmospheric dump valves (ADVs) (LCO 3.7.4, "Atmospheric Dump Valves (ADVs)"). If the main condenser is available, steam may be released via the steam bypass valves and recirculated to the CST.

The AFW System consists of [two] motor driven AFW pumps and one steam turbine driven pump configured into three trains. Each motor driven pump provides 100% of AFW flow capacity; the turbine driven pump provides 100% of the required capacity to the steam generators as assumed in the accident analysis. The pumps are equipped with independent recirculation lines to prevent pump operation against a closed system.

Each motor driven AFW pump is powered from an independent Class 1E power supply, and feeds one steam generator, although each pump has the capability to be realigned from the control room to feed the other steam generator.

One pump at full flow is sufficient to remove decay heat and cool the unit to Shutdown Cooling (SDC) System entry conditions.

The steam turbine driven AFW pump receives steam from either main steam header upstream of the main steam isolation valve (MSIV). Each of the steam feed lines will supply 100% of the requirements of the turbine driven AFW pump. The turbine driven AFW pump supplies a common header capable of feeding both steam generators, with DC powered control valves actuated to the appropriate steam generator by the Emergency Feedwater Actuation System (EFAS).

The AFW System supplies feedwater to the steam generators during normal unit startup, shutdown, and hot standby conditions.

BASES

BACKGROUND (continued)

The AFW System is designed to supply sufficient water to the steam generator(s) to remove decay heat with steam generator pressure at the setpoint of the MSSVs. Subsequently, the AFW System supplies sufficient water to cool the unit to SDC entry conditions, and steam is released through the ADVs.

The AFW System actuates automatically on low steam generator level by the EFAS as described in LCO 3.3.2, "Engineered Safety Feature Actuation System (ESFAS) Instrumentation." The EFAS logic is designed to feed either or both steam generators with low levels, but will isolate the AFW System from a steam generator having a significantly lower steam pressure than the other steam generator. The EFAS automatically actuates the AFW turbine driven pump and associated DC operated valves and controls when required, to ensure an adequate feedwater supply to the steam generators. DC operated valves are provided for each AFW line to control the AFW flow to each steam generator.

The AFW System is discussed in the FSAR, Section [10.4.9] (Ref. 1).

APPLICABLE SAFETY ANALYSES

The AFW System mitigates the consequences of any event with a loss of normal feedwater.

The design basis of the AFW System is to supply water to the steam generator to remove decay heat and other residual heat, by delivering at least the minimum required flow rate to the steam generators at pressures corresponding to the lowest MSSV set pressure plus 3%.

The limiting Design Basis Accidents (DBAs) and transients for the AFW System are as follows:

a. Feedwater Line Break (FWLB) and

b. Loss of normal feedwater.

In addition, the minimum available AFW flow and system characteristics are serious considerations in the analysis of a small break loss of coolant accident.

BASES

APPLICABLE SAFETY ANALYSES (continued)

The AFW System design is such that it can perform its function following an FWLB between the MFW isolation valve and containment, combined with a loss of offsite power following turbine trip, and a single active failure of the steam turbine driven AFW pump. In such a case, the EFAS logic might not detect the affected steam generator if the backflow check valve to the affected MFW header worked properly. One motor driven AFW pump would deliver to the broken MFW header at the pump runout flow until the problem was detected, and flow was terminated by the operator. Sufficient flow would be delivered to the intact steam generator by the redundant AFW pump.

The AFW System satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

This LCO requires that [three] AFW trains be OPERABLE to ensure that the AFW System will perform the design safety function to mitigate the consequences of accidents that could result in overpressurization of the reactor coolant pressure boundary. Three independent AFW pumps, in two diverse trains, ensure availability of residual heat removal capability for all events accompanied by a loss of offsite power and a single failure. This is accomplished by powering two pumps from independent emergency buses. The third AFW pump is powered by a diverse means, a steam driven turbine supplied with steam from a source not isolated by the closure of the MSIVs.

The AFW System is considered to be OPERABLE when the components and flow paths required to provide AFW flow to the steam generators are OPERABLE. This requires that the two motor driven AFW pumps be OPERABLE in two diverse paths, each supplying AFW to a separate steam generator. The turbine driven AFW pump shall be OPERABLE with redundant steam supplies from each of the two main steam lines upstream of the MSIVs and capable of supplying AFW flow to either of the two steam generators. The piping, valves, instrumentation, and controls in the required flow paths shall also be OPERABLE.

The LCO is modified by a Note indicating that only one AFW train, which includes a motor driven pump, is required to be OPERABLE in MODE 4. This is because of reduced heat removal requirements, the short period of time in MODE 4 during which AFW is required, and the insufficient steam supply available in MODE 4 to power the turbine driven AFW pump.

BASES

APPLICABILITY

In MODES 1, 2, and 3, the AFW System is required to be OPERABLE and to function in the event that the MFW is lost. In addition, the AFW System is required to supply enough makeup water to replace steam generator secondary inventory, lost as the unit cools to MODE 4 conditions.

In MODE 4, the AFW System may be used for heat removal via the steam generator.

In MODES 5 and 6, the steam generators are not normally used for decay heat removal, and the AFW System is not required.

ACTIONS

A Note prohibits the application of LCO 3.0.4.b to an inoperable AFW train. There is an increased risk associated with entering a MODE or other specified condition in the Applicability with an AFW train inoperable and the provisions of LCO 3.0.4.b, which allow entry into a MODE or other specified condition in the Applicability with the LCO not met after performance of a risk assessment addressing inoperable systems and components, should not be applied in this circumstance.

[A.1

If one of the two steam supplies to the turbine driven AFW pumps is inoperable, or if a turbine driven pump is inoperable while in MODE 3 immediately following refueling, action must be taken to restore the inoperable equipment to an OPERABLE status within 7 days. The 7 day Completion Time is reasonable based on the following reasons:

a. For the inoperability of a steam supply to the turbine driven AFW pump, the 7 day Completion Time is reasonable since there is a redundant steam supply line for the turbine driven pump.

b. For the inoperability of a turbine driven AFW pump while in MODE 3 immediately subsequent to a refueling outage, the 7 day Completion Time is reasonable due to the minimal decay heat levels in this situation.

c. For both the inoperability of a steam supply line to the turbine driven pump and an inoperable turbine driven AFW pump while in MODE 3 immediately following a refueling outage, the 7 day Completion Time is reasonable due to the availability of redundant OPERABLE motor driven AFW pumps; and due to the low probability of an event requiring the use of the turbine driven AFW pump.

BASES

ACTIONS (continued)

Condition A is modified by a Note which limits the applicability of the Condition to when the unit has not entered MODE 2 following a refueling. Condition A allows one AFW train to be inoperable for 7 days vice the 72 hour Completion Time in Condition B. This longer Completion Time is based on the reduced decay heat following refueling and prior to the reactor being critical.]

<u>B.1</u>

With one of the required AFW trains (pump or flow path) inoperable, action must be taken to restore OPERABLE status within 72 hours. This Condition includes the loss of two steam supply lines to the turbine driven AFW pump. The 72 hour Completion Time is reasonable based on the redundant capabilities afforded by the AFW System, the time needed for repairs, and the low probability of a DBA event occurring during this period. Two AFW pumps and flow paths remain to supply feedwater to the steam generators.

<u>C.1 and C.2</u>

When either Required Action A.1 or B.1 cannot be completed within the required Completion Time, [or if two AFW trains are inoperable in MODES 1, 2, and 3], the unit must be placed in a MODE in which the LCO does not apply. To achieve this status, the unit must be placed in at least MODE 3 within 6 hours, and in MODE 4 within [18] hours.

The allowed Completion Times are reasonable, based on operating experience, to reach the required unit conditions from full power conditions in an orderly manner and without challenging unit systems.

In MODE 4, with [two AFW trains inoperable in MODES 1, 2, and 3], operation is allowed to continue because only one motor driven AFW pump is required in accordance with the Note that modifies the LCO. Although it is not required, the unit may continue to cool down and start the SDC.

BASES

ACTIONS (continued)

D.1

Required Action D.1 is modified by a Note indicating that all required MODE changes or power reductions are suspended until one AFW train is restored to OPERABLE status.

With all [three] AFW trains inoperable in MODES 1, 2, and 3, the unit is in a seriously degraded condition with no safety related means for conducting a cooldown, and only limited means for conducting a cooldown with nonsafety grade equipment. In such a condition, the unit should not be perturbed by any action, including a power change, that might result in a trip. The seriousness of this condition requires that action be started immediately to restore one AFW train to OPERABLE status. LCO 3.0.3 is not applicable, as it could force the unit into a less safe condition.

E.1

Required Action E.1 is modified by a Note indicating that all required MODE changes or power reductions are suspended until one AFW train is restored to OPERABLE status.

With one AFW train inoperable, action must be taken to immediately restore the inoperable train to OPERABLE status or to immediately verify, by administrative means, the OPERABILITY of a second train. LCO 3.0.3 is not applicable, as it could force the unit into a less safe condition.

In MODE 4, either the reactor coolant pumps or the SDC loops can be used to provide forced circulation as discussed in LCO 3.4.6, "RCS Loops - MODE 4."

SURVEILLANCE REQUIREMENTS

SR 3.7.5.1

Verifying the correct alignment for manual, power operated, and automatic valves in the AFW water and steam supply flow paths provides assurance that the proper flow paths exist for AFW operation. This SR does not apply to valves that are locked, sealed, or otherwise secured in position, since these valves are verified to be in the correct position prior to locking, sealing, or securing. This SR also does not apply to valves that cannot be inadvertently misaligned, such as check valves. This Surveillance does not require any testing or valve manipulations; rather, it involves verification that those valves capable of potentially being mispositioned are in the correct position.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The 31 day Frequency is based on engineering judgment, is consistent with the procedural controls governing valve operation, and ensures correct valve positions.

SR 3.7.5.2

Verifying that each AFW pump's developed head at the flow test point is greater than or equal to the required developed head ensures that AFW pump performance has not degraded during the cycle. Flow and differential head are normal tests of pump performance required by the ASME Code (Ref. 2). Because it is undesirable to introduce cold AFW into the steam generators while they are operating, this testing is performed on recirculation flow. This test confirms one point on the pump design curve and is indicative of overall performance. Such inservice tests confirm component OPERABILITY, trend performance, and detect incipient failures by indicating abnormal performance. Performance of inservice testing, discussed in the ASME Code (Ref. 2), at 3 month intervals satisfies this requirement.

This SR is modified by a Note indicating that the SR should be deferred until suitable test conditions are established. This deferral is required because there is an insufficient steam pressure to perform the test.

SR 3.7.5.3

This SR ensures that AFW can be delivered to the appropriate steam generator, in the event of any accident or transient that generates an EFAS signal, by demonstrating that each automatic valve in the flow path actuates to its correct position on an actual or simulated actuation signal. This Surveillance is not required for valves that are locked, sealed, or otherwise secured in the required position under administrative controls. The [18] month Frequency is based on the need to perform this Surveillance under the conditions that apply during a unit outage and the potential for an unplanned transient if the Surveillance were performed with the reactor at power. The 18 month Frequency is acceptable, based on the design reliability and operating experience of the equipment.

This SR is modified by a Note indicating that the SR should be deferred until suitable test conditions have been established. This deferral is required because there is an insufficient steam pressure to perform the test.

BASES

SURVEILLANCE REQUIREMENTS (continued)

Also, this SR is modified by a Note that states the SR is not required to be met in MODE 4. In MODE 4, the required AFW train is already aligned and operating.

SR 3.7.5.4

This SR ensures that the AFW pumps will start in the event of any accident or transient that generates an EFAS signal by demonstrating that each AFW pump starts automatically on an actual or simulated actuation signal. The [18] month Frequency is based on the need to perform this Surveillance under the conditions that apply during a unit outage and the potential for an unplanned transient if the Surveillance were performed with the reactor at power. The 18 month Frequency is acceptable, based on the design reliability and operating experience of the equipment.

[This SR is modified by two Notes. Note 1 indicates that the SR be deferred until suitable test conditions are established. This deferral is required because there is insufficient steam pressure to perform the test. Note 2 states that the SR is not required to be met in MODE 4. [In MODE 4, the required pump is already operating and the autostart function is not required.] [In MODE 4, the heat removal requirements would be less providing more time for operator action to manually start the required AFW pump.]

----------------------------------REVIEWER'S NOTE----------------------------------
Some plants may not routinely use the AFW for heat removal in MODE 4. The second justification is provided for plants that use a startup feedwater pump rather than AFW for startup and shutdown.

SR 3.7.5.5

This SR ensures that the AFW System is properly aligned by verifying the flow path to each steam generator prior to entering MODE 2 operation, after 30 days in any combination of MODE 5 or 6, or defueled. OPERABILITY of AFW flow paths must be verified before sufficient core heat is generated that would require the operation of the AFW System during a subsequent shutdown. The Frequency is reasonable, based on engineering judgment, and other administrative controls to ensure that flow paths remain OPERABLE. To further ensure AFW System alignment, the OPERABILITY of the flow paths is verified following

BASES

SURVEILLANCE REQUIREMENTS (continued)

extended outages to determine that no misalignment of valves has occurred. This SR ensures that the flow path from the CST to the steam generators is properly aligned by requiring a verification of minimum flow capacity of 750 gpm at 1270 psi. (This SR is not required by those units that use AFW for normal startup and shutdown.)

REFERENCES

1. FSAR, Section [10.4.9].

2. ASME Code for Operation and Maintenance of Nuclear Power Plants.

B 3.7 PLANT SYSTEMS

B 3.7.6 Condensate Storage Tank (CST)

BASES

BACKGROUND

The CST provides a safety grade source of water to the steam generators for removing decay and sensible heat from the Reactor Coolant System (RCS). The CST provides a passive flow of water, by gravity, to the Auxiliary Feedwater (AFW) System (LCO 3.7.4, "Auxiliary Feedwater (AFW) System"). The steam produced is released to the atmosphere by the main steam safety valves (MSSVs) or the atmospheric dump valves. The AFW pumps operate with a continuous recirculation to the CST.

When the main steam isolation valves are open, the preferred means of heat removal is to discharge steam to the condenser by the nonsafety grade path of the steam bypass valves. The condensed steam is returned to the CST by the condensate transfer pump. This has the advantage of conserving condensate while minimizing releases to the environment.

Because the CST is a principal component in removing residual heat from the RCS, it is designed to withstand earthquakes and other natural phenomena. The CST is designed to Seismic Category I requirements to ensure availability of the feedwater supply. Feedwater is also available from an alternate source.

A description of the CST is found in the FSAR, Section [9.2.6] (Ref. 1).

APPLICABLE SAFETY ANALYSES

The CST provides cooling water to remove decay heat and to cool down the unit following all events in the accident analysis, discussed in the FSAR, Chapters [6] and [15] (Refs. 2 and 3, respectively). For anticipated operational occurrences and accidents which do not affect the OPERABILITY of the steam generators, the analysis assumption is generally [30] minutes at MODE 3, steaming through the MSSVs followed by a cooldown to shutdown cooling (SDC) entry conditions at the design cooldown rate.

The limiting event for the condensate volume is the large feedwater line break with a coincident loss of offsite power. Single failures that also affect this event include the following:

a. The failure of the diesel generator powering the motor driven AFW pump to the unaffected steam generator (requiring additional steam to drive the remaining AFW pump turbine) and

BASES

APPLICABLE SAFETY ANALYSES (continued)

b. The failure of the steam driven AFW pump (requiring a longer time for cooldown using only one motor driven AFW pump).

These are not usually the limiting failures in terms of consequences for these events.

A nonlimiting event considered in CST inventory determinations is a break either in the main feedwater, or AFW line near where the two join. This break has the potential for dumping condensate until terminated by operator action, as the Emergency Feedwater Actuation System would not detect a difference in pressure between the steam generators for this break location. This loss of condensate inventory is partially compensated by the retaining of steam generator inventory.

The CST satisfies Criteria 2 and 3 of 10 CFR 50.36(c)(2)(ii).

LCO

To satisfy accident analysis assumptions, the CST must contain sufficient cooling water to remove decay heat for [30 minutes] following a reactor trip from 102% RTP, and then cool down the RCS to SDC entry conditions, assuming a coincident loss of offsite power and the most adverse single failure. In doing this it must retain sufficient water to ensure adequate net positive suction head for the AFW pumps during the cooldown, as well as to account for any losses from the steam driven AFW pump turbine, or before isolating AFW to a broken line.

The CST level required is a usable volume of ≤ [350,000] gallons, which is based on holding the unit in MODE 3 for [4] hours, followed by a cooldown to SDC entry conditions at 75°F per hour. This basis is established by the NRC Standard Review Plan Branch Technical Position, Reactor Systems Branch 5-1 (Ref. 4) and exceeds the volume required by the accident analysis.

OPERABILITY of the CST is determined by maintaining the tank level at or above the minimum required level.

APPLICABILITY

In MODES 1, 2, and 3, [and in MODE 4, when steam generator is being relied upon for heat removal,] the CST is required to be OPERABLE.

In MODES 5 and 6, the CST is not required because the AFW System is not required.

BASES

ACTIONS

A.1 and A.2

If the CST is not OPERABLE, the OPERABILITY of the backup water supply must be verified by administrative means within 4 hours and once every 12 hours thereafter.

OPERABILITY of the backup feedwater supply must include verification of the OPERABILITY of flow paths from the backup supply to the AFW pumps, and availability of the required volume of water in the backup supply. The CST must be returned to OPERABLE status within 7 days, as the backup supply may be performing this function in addition to its normal functions. The 4 hour Completion Time is reasonable, based on operating experience, to verify the OPERABILITY of the backup water supply. Additionally, verifying the backup water supply every 12 hours is adequate to ensure the backup water supply continues to be available. The 7 day Completion Time is reasonable, based on an OPERABLE backup water supply being available, and the low probability of an event requiring the use of the water from the CST occurring during this period.

B.1 and B.2

If the CST cannot be restored to OPERABLE status within the associated Completion Time, the unit must be placed in a MODE in which the LCO does not apply. To achieve this status, the unit must be placed in at least MODE 3 within 6 hours, and in MODE 4, without reliance on steam generator for heat removal, within [24] hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required unit conditions from full power conditions in an orderly manner and without challenging unit systems.

SURVEILLANCE REQUIREMENTS

SR 3.7.6.1

This SR verifies that the CST contains the required volume of cooling water. (This level ≥ [350,000] gallons.) The 12 hour Frequency is based on operating experience, and the need for operator awareness of unit evolutions that may affect the CST inventory between checks. The 12 hour Frequency is considered adequate in view of other indications in the control room, including alarms, to alert the operator to abnormal CST level deviations.

BASES

REFERENCES

1. FSAR, Section [9.2.6].
2. FSAR, Chapter [6].
3. FSAR, Chapter [15].
4. NRC Standard Review Plan Branch Technical Position RSB 5-1.

B 3.7 PLANT SYSTEMS

B 3.7.7 Component Cooling Water (CCW) System

BASES

BACKGROUND

The CCW System provides a heat sink for the removal of process and operating heat from safety related components during a Design Basis Accident (DBA) or transient. During normal operation, the CCW System also provides this function for various nonessential components, as well as the spent fuel pool. The CCW System serves as a barrier to the release of radioactive byproducts between potentially radioactive systems and the Service Water System, and thus to the environment.

The CCW System is arranged as two independent full capacity cooling loops, and has isolatable nonsafety related components. Each safety related train includes a full capacity pump, surge tank, heat exchanger, piping, valves, and instrumentation. Each safety related train is powered from a separate bus. An open surge tank in the system provides pump trip protective functions to ensure sufficient net positive suction head is available. The pump in each train is automatically started on receipt of a safety injection actuation signal, and all nonessential components are isolated.

Additional information on the design and operation of the system, along with a list of the components served, is presented in the FSAR, Section [9.2.2], Reference 1. The principal safety related function of the CCW System is the removal of decay heat from the reactor via the Shutdown Cooling (SDC) System heat exchanger. This may utilize the SCS heat exchanger, during a normal or post accident cooldown and shutdown, or the Containment Spray System during the recirculation phase following a loss of coolant accident (LOCA).

APPLICABLE SAFETY ANALYSES

The design basis of the CCW System is for one CCW train in conjunction with a 100% capacity Containment Cooling System (containment spray, containment coolers, or a combination) removing core decay heat 20 minutes after a design basis LOCA. This prevents the containment sump fluid from increasing in temperature during the recirculation phase following a LOCA, and provides a gradual reduction in the temperature of this fluid as it is supplied to the Reactor Coolant System (RCS) by the safety injection pumps.

The CCW System is designed to perform its function with a single failure of any active component, assuming a loss of offsite power.

BASES

APPLICABLE SAFETY ANALYSES (continued)

The CCW System also functions to cool the unit from SDC entry conditions (T_{cold} < [350]°F) to MODE 5 (T_{cold} < [200]°F) during normal and post accident operations. The time required to cool from [350]°F to [200]°F is a function of the number of CCW and SDC trains operating. One CCW train is sufficient to remove decay heat during subsequent operations with T_{cold} < [200]°F. This assumes that a maximum seawater temperature of 76°F occurs simultaneously with the maximum heat loads on the system.

The CCW System satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

The CCW trains are independent of each other to the degree that each has separate controls and power supplies and the operation of one does not depend on the other. In the event of a DBA, one CCW train is required to provide the minimum heat removal capability assumed in the safety analysis for the systems to which it supplies cooling water. To ensure this requirement is met, two CCW trains must be OPERABLE. At least one CCW train will operate assuming the worst single active failure occurs coincident with the loss of offsite power.

A CCW train is considered OPERABLE when the following:

a. The associated pump and surge tank are OPERABLE and

b. The associated piping, valves, heat exchanger and instrumentation and controls required to perform the safety related function are OPERABLE.

The isolation of CCW from other components or systems not required for safety may render those components or systems inoperable, but does not affect the OPERABILITY of the CCW System.

APPLICABILITY

In MODES 1, 2, 3, and 4, the CCW System is a normally operating system that must be prepared to perform its post accident safety functions, primarily RCS heat removal by cooling the SDC heat exchanger.

In MODES 5 and 6, the OPERABILITY requirements of the CCW System are determined by the systems it supports.

BASES

ACTIONS

A.1

Required Action A.1 is modified by a Note indicating the requirement of entry into the applicable Conditions and Required Actions of LCO 3.4.6, "RCS Loops - MODE 4," for SDC made inoperable by CCW. This is an exception to LCO 3.0.6 and ensures the proper actions are taken for these components.

With one CCW train inoperable, action must be taken to restore OPERABLE status within 72 hours. In this Condition, the remaining OPERABLE CCW train is adequate to perform the heat removal function. The 72 hour Completion Time is based on the redundant capabilities afforded by the OPERABLE train, and the low probability of a DBA occurring during this period.

B.1 and B.2

If the CCW train cannot be restored to OPERABLE status within the associated Completion Time, the unit must be placed in a MODE in which the LCO does not apply. To achieve this status, the unit must be placed in at least MODE 3 within 6 hours and in MODE 5 within 36 hours.

The allowed Completion Times are reasonable, based on operating experience, to reach the required unit conditions from full power conditions in an orderly manner and without challenging unit systems.

SURVEILLANCE REQUIREMENTS

SR 3.7.7.1

Verifying the correct alignment for manual, power operated, and automatic valves in the CCW flow path provides assurance that the proper flow paths exist for CCW operation. This SR does not apply to valves that are locked, sealed, or otherwise secured in position, since these valves are verified to be in the correct position prior to locking, sealing, or securing. This SR also does not apply to valves that cannot be inadvertently misaligned, such as check valves. This Surveillance does not require any testing or valve manipulation; rather, it involves verification that those valves capable of potentially being mispositioned are in their correct position.

This SR is modified by a Note indicating that the isolation of the CCW components or systems may render those components inoperable but does not affect the OPERABILITY of the CCW System.

The 31 day Frequency is based on engineering judgment, is consistent with the procedural controls governing valve operation, and ensures correct valve positions.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.7.7.2

This SR verifies proper automatic operation of the CCW valves on an actual or simulated actuation signal. The CCW System is a normally operating system that cannot be fully actuated as part of routine testing during normal operation. This Surveillance is not required for valves that are locked, sealed, or otherwise secured in the required position under administrative controls. The [18] month Frequency is based on the need to perform this Surveillance under the conditions that apply during a unit outage and the potential for an unplanned transient if the Surveillance were performed with the reactor at power. Operating experience has shown that these components usually pass the Surveillance when performed at the [18] month Frequency. Therefore, the Frequency is acceptable from a reliability standpoint.

SR 3.7.7.3

This SR verifies proper automatic operation of the CCW pumps on an actual or simulated actuation signal. The CCW System is a normally operating system that cannot be fully actuated as part of routine testing during normal operation. The [18] month Frequency is based on the need to perform this Surveillance under the conditions that apply during a unit outage and the potential for an unplanned transient if the Surveillance were performed with the reactor at power. Operating experience has shown these components usually pass the Surveillance when performed at the [18] month Frequency. Therefore, the Frequency is acceptable from a reliability standpoint.

REFERENCES

1. FSAR, Section [9.2.2].

B 3.7 PLANT SYSTEMS

B 3.7.8 Service Water System (SWS)

BASES

BACKGROUND	The SWS provides a heat sink for the removal of process and operating heat from safety related components during a Design Basis Accident (DBA) or transient. During normal operation or a normal shutdown, the SWS also provides this function for various safety related and nonsafety related components. The safety related function is covered by this LCO. The SWS consists of two separate, 100% capacity safety related cooling water trains. Each train consists of two 100% capacity pumps, one component cooling water (CCW) heat exchanger, piping, valves, instrumentation, and two cyclone separators. The pumps and valves are remote manually aligned, except in the unlikely event of a loss of coolant accident (LOCA). The pumps aligned to the critical loops are automatically started upon receipt of a safety injection actuation signal and all essential valves are aligned to their post accident positions. The SWS also provides emergency makeup to the spent fuel pool and CCW System [and is the backup water supply to the Auxiliary Feedwater System]. Additional information about the design and operation of the SWS, along with a list of the components served, is presented in the FSAR, Section [9.2.1] (Ref. 1). The principal safety related function of the SWS is the removal of decay heat from the reactor via the [CCW System].
APPLICABLE SAFETY ANALYSES	The design basis of the SWS is for one SWS train, in conjunction with the CCW System and a 100% capacity containment cooling system (containment spray, containment coolers, or a combination), removing core decay heat 20 minutes following a design basis LOCA, as discussed in the FSAR, Section [6.2] (Ref. 2). This prevents the containment sump fluid from increasing in temperature during the recirculation phase following a LOCA and provides for a gradual reduction in the temperature of this fluid as it is supplied to the Reactor Coolant System by the safety injection pumps. The SWS is designed to perform its function with a single failure of any active component, assuming the loss of offsite power. The SWS, in conjunction with the CCW System, also cools the unit from shutdown cooling (SDC), as discussed in the FSAR, Section [5.4.7] (Ref. 3) entry conditions to MODE 5 during normal and post accident operations. The time required for this evolution is a function of the

BASES

APPLICABLE SAFETY ANALYSES (continued)

number of CCW and SDC System trains that are operating. One SWS train is sufficient to remove decay heat during subsequent operations in MODES 5 and 6. This assumes that a maximum SWS temperature of 95°F occurring simultaneously with maximum heat loads on the system.

The SWS satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

Two SWS trains are required to be OPERABLE to provide the required redundancy to ensure that the system functions to remove post accident heat loads, assuming the worst single active failure occurs coincident with the loss of offsite power.

An SWS train is considered OPERABLE when:

a. The associated pump is OPERABLE and

b. The associated piping, valves, heat exchanger, and instrumentation and controls required to perform the safety related function are OPERABLE.

APPLICABILITY

In MODES 1, 2, 3, and 4, the SWS System is a normally operating system, which is required to support the OPERABILITY of the equipment serviced by the SWS and required to be OPERABLE in these MODES.

In MODES 5 and 6, the OPERABILITY requirements of the SWS are determined by the systems it supports.

ACTIONS

A.1

With one SSW train inoperable, action must be taken to restore OPERABLE status within 72 hours. In this Condition, the remaining OPERABLE SWS train is adequate to perform the heat removal function. However, the overall reliability is reduced because a single failure in the SWS train could result in loss of SWS function. Required Action A.1 is modified by two Notes. The first Note indicates that the applicable Conditions of LCO 3.8.1, "AC Sources - Operating," should be entered if the inoperable SWS train results in an inoperable emergency diesel generator. The second Note indicates that the applicable Conditions and Required Actions of LCO 3.4.6, "RCS Loops - MODE 4," should be entered if an inoperable SWS train results in an inoperable SDC. The 72 hour Completion Time is based on the redundant capabilities afforded by the OPERABLE train, and the low probability of a DBA occurring during this time period.

BASES

ACTIONS (continued)

B.1 and B.2

If the SWS train cannot be restored to OPERABLE status within the associated Completion Time, the unit must be placed in a MODE in which the LCO does not apply. To achieve this status, the unit must be placed in at least MODE 3 within 6 hours and in MODE 5 within 36 hours.

The allowed Completion Times are reasonable, based on operating experience, to reach the required unit conditions from full power conditions in an orderly manner and without challenging unit systems.

SURVEILLANCE REQUIREMENTS

SR 3.7.8.1

Verifying the correct alignment for manual, power operated, and automatic valves in the SWS flow path ensures that the proper flow paths exist for SWS operation. This SR does not apply to valves that are locked, sealed, or otherwise secured in position, since they are verified to be in the correct position prior to locking, sealing, or securing. This SR also does not apply to valves that cannot be inadvertently misaligned, such as check valves. This Surveillance does not require any testing or valve manipulation; rather, it involves verification that those valves capable of potentially being mispositioned are in the correct position. This SR is modified by a Note indicating that the isolation of the SWS components or systems may render those components inoperable but does not affect the OPERABILITY of the SWS.

The 31 day Frequency is based on engineering judgment, is consistent with the procedural controls governing valve operation, and ensures correct valve positions.

SR 3.7.8.2

This SR verifies proper automatic operation of the SWS valves on an actual or simulated actuation signal. The SWS is a normally operating system that cannot be fully actuated as part of the normal testing. This Surveillance is not required for valves that are locked, sealed, or otherwise secured in the required position under administrative controls. The [18] month Frequency is based on the need to perform this Surveillance under the conditions that apply during a unit outage and the potential for an unplanned transient if the Surveillance were performed with the reactor at power. Operating experience has shown that these components usually pass the Surveillance when performed at the [18] month Frequency. Therefore, the Frequency is acceptable from a reliability standpoint.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.7.8.3

The SR verifies proper automatic operation of the SWS pumps on an actual or simulated actuation signal. The SWS is a normally operating system that cannot be fully actuated as part of the normal testing during normal operation. The [18] month Frequency is based on the need to perform this Surveillance under the conditions that apply during a unit outage and the potential for an unplanned transient if the Surveillance were performed with the reactor at power. Operating experience has shown that these components usually pass the Surveillance when performed at the [18] month Frequency. Therefore, the Frequency is acceptable from a reliability standpoint.

REFERENCES

1. FSAR, Section [9.2.1].

2. FSAR, Section [6.2].

3. FSAR, Section [5.4.7].

B 3.7 PLANT SYSTEMS

B 3.7.9 Ultimate Heat Sink (UHS)

BASES

BACKGROUND

The UHS provides a heat sink for process and operating heat from safety related components during a Design Basis Accident (DBA) or transient, as well as during normal operation. This is done utilizing the Service Water System.

The UHS has been defined as that complex of water sources, including necessary retaining structures (e.g., a pond with its dam, or a river with its dam), and the canals or conduits connecting the sources with, but not including, the cooling water system intake structures as, discussed in the FSAR, Section [9.2.5] (Ref. 1). If cooling towers or portions thereof are required to accomplish the UHS safety functions, they should meet the same requirements as the sink. The two principal functions of the UHS are the dissipation of residual heat after reactor shutdown, and dissipation of residual heat after an accident.

A variety of complexes is used to meet the requirements for a UHS. A lake or an ocean may qualify as a single source. If the complex includes a water source contained by a structure, it is likely that a second source will be required.

The basic performance requirements are that a 30 day supply of water be available, and that the design basis temperatures of safety related equipment not be exceeded. Basins of cooling towers generally include less than a 30 day supply of water, typically 7 days or less. A 30 day supply would be dependent on another source(s) and a makeup system(s) for replenishing the source in the cooling tower basin. For smaller basin sources, which may be as small as a 1 day supply, the systems for replenishing the basin and the backup source(s) become of sufficient importance that the makeup system itself may be required to meet the same design criteria as an Engineered Safety Feature (e.g., single failure considerations, and multiple makeup water sources may be required).

It follows that the many variations in the UHS configurations will result in many unit to unit variations in OPERABILITY determinations and SRs. The ACTIONS and SRs are illustrative of a cooling tower UHS without a makeup requirement.

Additional information on the design and operation of the system along with a list of components served can be found in Reference 1.

BASES

APPLICABLE SAFETY ANALYSES	The UHS is the sink for heat removed from the reactor core following all accidents and anticipated operational occurrences in which the unit is cooled down and placed on shutdown cooling. For those units using it as the normal heat sink for condenser cooling via the Circulating Water System, unit operation at full power is its maximum heat load. Its maximum post accident heat load occurs 20 minutes after a design basis loss of coolant accident (LOCA). Near this time, the unit switches from injection to recirculation, and the containment cooling systems are required to remove the core decay heat. The operating limits are based on conservative heat transfer analyses for the worst case LOCA. Reference 1 provides the details of the assumptions used in the analysis. The assumptions include: worst expected meteorological conditions, conservative uncertainties when calculating decay heat, and the worst case failure (e.g., single failure of a manmade structure). The UHS is designed in accordance with Regulatory Guide 1.27 (Ref. 2), which requires a 30 day supply of cooling water in the UHS. The UHS satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).
LCO	The UHS is required to be OPERABLE. The UHS is considered OPERABLE if it contains a sufficient volume of water at or below the maximum temperature that would allow the SWS to operate for at least 30 days following the design basis LOCA without the loss of net positive suction head (NPSH), and without exceeding the maximum design temperature of the equipment served by the SWS. To meet this condition, the UHS temperature should not exceed [90]°F and the level should not fall below [562 ft mean sea level] during normal unit operation.
APPLICABILITY	In MODES 1, 2, 3, and 4, the UHS is a normally operating system that is required to support the OPERABILITY of the equipment serviced by the UHS and required to be OPERABLE in these MODES. In MODES 5 and 6, the OPERABILITY requirements of the UHS are determined by the systems it supports.

BASES

ACTIONS

[A.1

If one or more cooling towers have one fan inoperable (i.e., up to one fan per cooling tower inoperable), action must be taken to restored the inoperable cooling tower fan(s) to OPERABLE status within 7 days.

The 7 day Completion Time is reasonable, based on the low probability of an accident occurring during the 7 days that one cooling tower fan is inoperable, the number of available systems, and the time required to complete the action.]

[B.1

-----------------------------------REVIEWER'S NOTE-----------------------------------
The [ ]°F is the maximum allowed UHS temperature value and is based on temperature limitations of the equipment that is relied upon for accident mitigation and safe shutdown of the unit.

With water temperature of the UHS > [90]°F, the design basis assumption associated with initial UHS temperature are bounded provided the temperature of the UHS averaged over the previous 24 hour period is ≤ [90]°F. With the water temperature of the UHS > [90]°F, long term cooling capability of the ECCS loads and DGs may be affected. Therefore, to ensure long term cooling capability is provided to the ECCS loads when water temperature of the UHS is > [90]°F, Required Action B.1 is provided to more frequently monitor the water temperature of the UHS and verify the temperature is ≤ [90]°F when averaged over the previous 24 hour period. The once per hour Completion Time takes into consideration UHS temperature variations and the increased monitoring frequency needed to ensure design basis assumptions and equipment limitations are not exceeded in this condition. If the water temperature of the UHS exceeds [90]°F when averaged over the previous 24 hour period or the water temperature of the UHS exceeds [ ]°F, Condition C must be entered immediately.]

BASES

ACTIONS (continued)

[C.1 and C.2

If the Required Actions or Completion Times of Conditions [A or B] are not met, or the UHS is inoperable [for reasons other than Condition A or B], the unit must be placed in a MODE in which the LCO does not apply. To achieve this status, the unit must be placed in at least MODE 3 within 6 hours and in MODE 5 within 36 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required unit conditions from full power conditions in an orderly manner and without challenging unit systems.]

SURVEILLANCE REQUIREMENTS

[SR 3.7.9.1

This SR verifies adequate long term (30 days) cooling can be maintained. The level specified also ensures sufficient NPSH is available for operating the SWS pumps. The 24 hour Frequency is based on operating experience related to the trending of the parameter variations during the applicable MODES. This SR verifies that the UHS water level is ≥ [562] ft [mean sea level].]

[SR 3.7.9.2

This SR verifies that the SWS is available to cool the CCW System to at least its maximum design temperature within the maximum accident or normal design heat loads for 30 days following a DBA. The 24 hour Frequency is based on operating experience related to the trending of the parameter variations during the applicable MODES. This SR verifies that the UHS water temperature is ≤ [92]°F.]

[SR 3.7.9.3

Operating each cooling tower fan for ≥ [15] minutes verifies that all fans are OPERABLE and that all associated controls are functioning properly. It also ensures that fan or motor failure, or excessive vibration can be detected for corrective action. The 31 day Frequency is based on operating experience, the known reliability of the fan units, the redundancy available, and the low probability of significant degradation of the UHS cooling tower fans occurring between surveillances.]

REFERENCES

1. FSAR, Section [9.2.5].

2. Regulatory Guide 1.27.

B 3.7 PLANT SYSTEMS

B 3.7.10 Essential Chilled Water (ECW) System

BASES

BACKGROUND

The ECW System provides a heat sink for the removal of process and operating heat from selected safety related air handling systems during a Design Basis Accident (DBA) or transient.

The ECW System is a closed loop system consisting of two independent trains. Each 100% capacity train includes a heat exchanger, surge tank, pump, chemical addition tank, piping, valves, controls, and instrumentation. An independent 100% capacity chilled water refrigeration unit cools each train. The ECW System is actuated on a safety injection actuation signal (SIAS) and supplies chilled water to the heating, ventilation, and air conditioning (HVAC) units in Engineered Safety Feature (ESF) equipment areas (e.g., the main control room, electrical equipment room, and safety injection pump area).

The flow path for the ECW System includes the closed loop of piping to all serviced equipment, and branch lines up to the first normally closed isolation valve.

During normal operation, the normal HVAC System performs the cooling function of the ECW System. The normal HVAC System is a nonsafety grade system that automatically shuts down when the ECW System receives a start signal. Additional information about the design and operation of the system, along with a list of components served, can be found in the FSAR, Section [9.2.9] (Ref. 1).

APPLICABLE SAFETY ANALYSES

The design basis of the ECW System is to remove the post accident heat load from ESF spaces following a DBA coincident with a loss of offsite power. Each train provides chilled water to the HVAC units at the design temperature of 42°F and flow rate of 400 gpm.

The maximum heat load in the ESF pump room area occurs during the recirculation phase following a loss of coolant accident. During recirculation, hot fluid from the containment sump is supplied to the high pressure safety injection and containment spray pumps. This heat load to the area atmosphere must be removed by the ECW System to ensure that these pumps remain OPERABLE.

The ECW satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO

[Two] ECW trains are required to be OPERABLE to provide the required redundancy to ensure that the system functions to remove post accident heat loads, assuming the worst single failure.

An ECW train is considered OPERABLE when:

a. The associated pump and surge tank are OPERABLE and

b. The associated piping, valves, heat exchanger, refrigeration unit, and instrumentation and controls required to perform the safety related function are OPERABLE.

The isolation of the ECW from other components or systems may render those components or systems inoperable, but does not affect the OPERABILITY of the ECW System.

APPLICABILITY

In MODES 1, 2, 3, and 4, the ECW System is required to be OPERABLE when a LOCA or other accident would require ESF operation.

In MODES 5 and 6, potential heat loads are smaller and the probability of accidents requiring the ECW System is low.

ACTIONS

A.1

If one ECW train is inoperable, action must be taken to restore OPERABLE status within 7 days. In this condition, one OPERABLE ECW train is adequate to perform the cooling function. The 7 day Completion Time is reasonable, based on the low probability of an event occurring during this time, the 100% capacity OPERABLE ECW train, and the redundant availability of the normal HVAC System.

B.1 and B.2

If the ECW train cannot be restored to OPERABLE status within the associated Completion Time, the unit must be placed in a MODE in which the LCO does not apply. To achieve this status, the unit must be placed in at least MODE 3 within 6 hours, and in MODE 5 within 36 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required unit conditions from full power conditions in an orderly manner and without challenging unit systems.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.7.10.1

Verifying the correct alignment for manual, power operated, and automatic valves in the ECW flow path provides assurance that the proper flow paths exist for ECW operation. This SR does not apply to valves that are locked, sealed, or otherwise secured in position, since they are verified to be in the correct position prior to locking, sealing, or securing. This SR also does not apply to valves that cannot be inadvertently misaligned, such as check valves. This Surveillance does not require any testing or valve manipulation; rather, it involves verification that those valves capable of potentially being mispositioned are in the correct position.

This SR is modified by a Note indicating that the isolation of ECW flow to components or systems may render those components inoperable but does not affect the OPERABILITY of the ECW System.

The 31 day Frequency is based on engineering judgment, is consistent with the procedural controls governing valve operation, and ensures correct valve positions.

SR 3.7.10.2

This SR verifies proper automatic operation of the ECW System components that the ECW pumps will start in the event of any accident or transient that generates an SIAS. This SR also ensures that each automatic valve in the flow paths actuates to its correct position on an actual or simulated SIAS. The ECW System cannot be fully actuated as part of the SIAS CHANNEL FUNCTIONAL TEST during normal operation. The actuation logic is tested as part of the SIAS functional test every 92 days, except for the subgroup relays that actuate the system that cannot be tested during normal unit operation. The [18] month Frequency is based on the need to perform this Surveillance under the conditions that apply during a unit outage and the potential for an unplanned transient if the Surveillance were performed with the reactor at power. The [18] month Frequency is based on operating experience and design reliability of the equipment.

REFERENCES

1. FSAR, Section [9.2.9].

B 3.7 PLANT SYSTEMS

B 3.7.11 Control Room Emergency Air Cleanup System (CREACS)

BASES

BACKGROUND

The CREACS provides a protected environment from which operators can control the unit following an uncontrolled release of radioactivity, [chemicals, or toxic gas].

The CREACS consists of two independent, redundant trains that recirculate and filter the control room air. Each train consists of a prefilter and demister, a high efficiency particulate air (HEPA) filter, an activated charcoal adsorber section for removal of gaseous activity (principally iodine), and a fan. Ductwork, valves or dampers, and instrumentation also form part of the system, as do demisters that remove water droplets from the air stream. A second bank of HEPA filters follows the adsorber section to collect carbon fines, and to back up the main HEPA filter bank if it fails.

The CREACS is an emergency system, part of which may also operate during normal unit operations in the standby mode of operation. Upon receipt of the actuating signal(s), normal air supply to the control room is isolated, and the stream of ventilation air is recirculated through the filter trains of the system. The prefilters and demisters remove any large particles in the air, and any entrained water droplets present to prevent excessive loading of the HEPA filters and charcoal adsorbers. Continuous operation of each train for at least 10 hours per month with the heaters on reduces moisture buildup on the HEPA filters and adsorbers. Both the demister and heater are important to the effectiveness of the charcoal adsorbers.

Actuation of the CREACS places the system into either of two separate states of the emergency mode of operation, depending on the initiation signal. Actuation of the system to the emergency radiation state of the emergency mode of operation closes the unfiltered outside air intake and unfiltered exhaust dampers, and aligns the system for recirculation of control room air through the redundant trains of HEPA and charcoal filters. The emergency radiation state initiates pressurization and filtered ventilation of the air supply to the control room.

Outside air is filtered, [diluted with building air from the electrical equipment and cable spreading rooms,] and then added to the air being recirculated from the control room. Pressurization of the control room prevents infiltration of unfiltered air from the surrounding areas of the

BASES

BACKGROUND (continued)

building. The actions taken in the toxic gas isolation state are the same, except that the signal switches control room ventilation to an isolation mode, preventing outside air from entering the control room.

The air entering the control room is continuously monitored by radiation and toxic gas detectors. One detector output above the setpoint will cause actuation of the emergency radiation state or toxic gas isolation state as required. The actions of the toxic gas isolation state are more restrictive, and will override the actions of the emergency radiation state.

A single train will pressurize the control room to about [0.125] inches water gauge, and provides an air exchange rate in excess of 25% per hour. The CREACS operation in maintaining the control room habitable is discussed in the FSAR, Section [9.4] (Ref. 1).

Redundant supply and recirculation trains provide the required filtration should an excessive pressure drop develop across the other filter train. Normally open isolation dampers are arranged in series pairs so that the failure of one damper to shut will not result in a breach of isolation. The CREACS is designed in accordance with Seismic Category I requirements.

The CREACS is designed to maintain the control room environment for 30 days of continuous occupancy after a Design Basis Accident (DBA) without exceeding a 5 rem whole body dose or its equivalent to any part of the body.

APPLICABLE SAFETY ANALYSES

The CREACS components are arranged in redundant safety related ventilation trains. The location of components and ducting within the control room envelope ensures an adequate supply of filtered air to all areas requiring access.

The CREACS provides airborne radiological protection for the control room operators, as demonstrated by the control room accident dose analyses for the most limiting design basis loss of coolant accident fission product release presented in the FSAR, Chapter [15] (Ref. 2).

The analysis of toxic gas releases demonstrates that the toxicity limits are not exceeded in the control room following a toxic chemical release, as presented in Reference 1.

The worst case single active failure of a component of the CREACS, assuming a loss of offsite power, does not impair the ability of the system to perform its design function.

The CREACS satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

BASES (continued)

LCO

Two independent and redundant trains of the CREACS are required to be OPERABLE to ensure that at least one is available, assuming that a single failure disables the other train. Total system failure could result in a control room operator receiving a dose in excess of 5 rem in the event of a large radioactive release.

The CREACS is considered OPERABLE when the individual components necessary to control operator exposure are OPERABLE in both trains. A CREACS train is considered OPERABLE when the associated:

a. Fan is OPERABLE,

b. HEPA filters and charcoal adsorber are not excessively restricting flow, and are capable of performing their filtration functions, and

c. Heater, demister, ductwork, valves, and dampers are OPERABLE, and air circulation can be maintained.

In addition, the control room boundary must be maintained, including the integrity of the walls, floors, ceilings, ductwork, and access doors.

The LCO is modified by a Note allowing the control room boundary to be opened intermittently under administrative controls. For entry and exit through doors, the administrative control of the opening is performed by the person(s) entering or exiting the area. For other openings, these controls consist of stationing a dedicated individual at the opening who is in continuous communication with the control room. This individual will have a method to rapidly close the opening when a need for control room isolation is indicated.

APPLICABILITY

In MODES 1, 2, 3, and 4, the CREACS must be OPERABLE to limit operator exposure during and following a DBA.

In MODES [5 and 6], the CREACS is required to cope with the release from a rupture of an outside waste gas tank.

During movement of [recently] irradiated fuel assemblies, the CREACS must be OPERABLE to cope with the release from a fuel handling accident. [Due to radioactive decay, CREACS is only required to cope with fuel handling accidents involving handling recently irradiated fuel (i.e., fuel that has occupied part of a critical reactor core within the previous [X] days).]

BASES

ACTIONS

A.1

With one CREACS train inoperable, action must be taken to restore OPERABLE status within 7 days. In this Condition, the remaining OPERABLE CREACS subsystem is adequate to perform control room radiation protection function. However, the overall reliability is reduced because a single failure in the OPERABLE CREACS train could result in loss of CREACS function. The 7 day Completion Time is based on the low probability of a DBA occurring during this time period, and the ability of the remaining train to provide the required capability.

B.1

-----------------------------------REVIEWER'S NOTE-----------------------------------
Adoption of Condition B is dependent on a commitment from the licensee to have written procedures available describing compensatory measures to be taken in the event of an intentional or unintentional entry into Condition B.

If the control room boundary is inoperable in MODES 1, 2, 3, and 4, the CREACS trains cannot perform their intended functions. Actions must be taken to restore an OPERABLE control room boundary within 24 hours. During the period that the control room boundary is inoperable, appropriate compensatory measures (consistent with the intent of GDC 19) should be utilized to protect control room operators from potential hazards such as radioactive contamination, toxic chemicals, smoke, temperature and relative humidity, and physical security. Preplanned measures should be available to address these concerns for intentional and unintentional entry into the condition. The 24 hour Completion Time is reasonable based on the low probability of a DBA occurring during this time period, and the use of compensatory measures. The 24 hour Completion Time is a typically reasonable time to diagnose, plan and possibly repair, and test most problems with the control room boundary.

C.1 and C.2

If the inoperable CREACS or control room boundary cannot be restored to OPERABLE status within the associated Completion Time in MODE 1, 2, 3, or 4, the unit must be placed in a MODE that minimizes the accident risk. To achieve this status, the unit must be placed in at least MODE 3 within 6 hours, and in MODE 5 within 36 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required unit conditions from full power conditions in an orderly manner and without challenging unit systems.

BASES

ACTIONS (continued)

D.1 and D.2

Required Action D.1 is modified by a Note indicating to place the system in the emergency radiation protection mode if the automatic transfer to emergency mode is inoperable.

In MODE 5 or 6, or during movement of [recently] irradiated fuel assemblies, if Required Action A.1 cannot be completed within the required Completion Time, the OPERABLE CREACS train must be immediately placed in the emergency mode of operation. This action ensures that the remaining train is OPERABLE, that no failures preventing automatic actuation will occur, and that any active failure will be readily detected.

An alternative to Required Action D.1 is to immediately suspend activities that could result in a release of radioactivity that might require isolation of the control room. This places the unit in a condition that minimizes the accident risk. This does not preclude the movement of fuel assemblies to a safe position.

E.1

When [in MODES 5 and 6, or] during movement of [recently] irradiated fuel assemblies, with two CREACS trains inoperable, action must be taken immediately to suspend activities that could result in a release of radioactivity that might require isolation of the control room. This places the unit in a condition that minimizes the accident risk. This does not preclude the movement of fuel to a safe position.

F.1

If both CREACS trains are inoperable in MODE 1, 2, 3, or 4 for reasons other than an inoperable control room boundary (i.e., Condition B), the CREACS may not be capable of performing the intended function and the unit is in a condition outside the accident analyses. Therefore, LCO 3.0.3 must be entered immediately.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.7.11.1

Standby systems should be checked periodically to ensure that they function properly. Since the environment and normal operating conditions on this system are not severe, testing each train once every month provides an adequate check on this system.

Monthly heater operations dry out any moisture accumulated in the charcoal from humidity in the ambient air. [Systems with heaters must be operated for ≥ 10 continuous hours with the heaters energized. Systems without heaters need only be operated for ≥ 15 minutes to demonstrate the function of the system.] The 31 day Frequency is based on the known reliability of the equipment, and the two train redundancy available.

SR 3.7.11.2

This SR verifies that the required CREACS testing is performed in accordance with the [Ventilation Filter Testing Program (VFTP)]. The [VFTP] includes testing HEPA filter performance, charcoal adsorber efficiency, minimum system flow rate, and the physical properties of the activated charcoal (general use and following specific operations). Specific test frequencies and additional information are discussed in detail in the [VFTP].

SR 3.7.11.3

This SR verifies each CREACS train starts and operates on an actual or simulated actuation signal. The Frequency of [18] months is consistent with that specified in Reference 3.

SR 3.7.11.4

This SR verifies the integrity of the control room enclosure and the assumed inleakage rates of potentially contaminated air. The control room positive pressure, with respect to potentially contaminated adjacent areas, is periodically tested to verify proper function of the CREACS. During the emergency radiation state of the emergency mode of operation, the CREACS is designed to pressurize the control room ≥ [0.125] inches water gauge positive pressure with respect to adjacent areas in order to prevent unfiltered inleakage. The CREACS is designed to maintain this positive pressure with one train at an emergency ventilation flow rate of [3000] cfm. The Frequency of [18] months on a STAGGERED TEST BASIS is consistent with the guidance provided in NUREG-0800, Section 6.4 (Ref. 4).

BASES

REFERENCES

1. FSAR, Section [9.4].
2. FSAR, Chapter [15].
3. Regulatory Guide 1.52, Rev. [2].
4. NUREG-0800, Section 6.4, Rev. 2, July 1981.

B 3.7 PLANT SYSTEMS

B 3.7.12 Control Room Emergency Air Temperature Control System (CREATCS)

BASES

BACKGROUND

The CREATCS provides temperature control for the control room following isolation of the control room.

The CREATCS consists of two independent, redundant trains that provide cooling and heating of recirculated control room air. Each train consists of heating coils, cooling coils, instrumentation, and controls to provide for control room temperature control.

The CREATCS is an emergency system, parts of which may also operate during normal unit operations. A single train will provide the required temperature control to maintain the control room between [70]°F and [85]°F. The CREATCS operation to maintain the control room temperature is discussed in the FSAR, Section [6.4] (Ref. 1).

APPLICABLE SAFETY ANALYSES

The design basis of the CREATCS is to maintain temperature of the control room environment throughout 30 days of continuous occupancy.

The CREATCS components are arranged in redundant safety related trains. During emergency operation, the CREATCS maintains the temperature between [70]°F and [85]°F. A single active failure of a component of the CREATCS, assuming a loss of offsite power, does not impair the ability of the system to perform its design function. Redundant detectors and controls are provided for control room temperature control. The CREATCS is designed in accordance with Seismic Category I requirements. The CREATCS is capable of removing sensible and latent heat loads from the control room, considering equipment heat loads and personnel occupancy requirements, to ensure equipment OPERABILITY.

The CREATCS satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

Two independent and redundant trains of the CREATCS are required to be OPERABLE to ensure that at least one is available, assuming a single failure disables the other train. Total system failure could result in the equipment operating temperature exceeding limits in the event of an accident.

The CREATCS is considered OPERABLE when the individual components that are necessary to maintain the control room temperature are OPERABLE in both trains. These components include the cooling coils and associated temperature control instrumentation. In addition, the CREATCS must be OPERABLE to the extent that air circulation can be maintained.

BASES

APPLICABILITY

In MODES 1, 2, 3, 4, [5, and 6,] and during movement of [recently] irradiated fuel assemblies [(i.e., fuel that has occupied part of a critical reactor core within the previous [X] days)], the CREATCS must be OPERABLE to ensure that the control room temperature will not exceed equipment OPERABILITY requirements following isolation of the control room.

In MODES 5 and 6, CREATCS may not be required for those facilities which do not require automatic control room isolation.

ACTIONS

A.1

With one CREATCS train inoperable, action must be taken to restore OPERABLE status within 30 days. In this Condition, the remaining OPERABLE CREATCS train is adequate to maintain the control room temperature within limits. The 30 day Completion Time is reasonable, based on the low probability of an event occurring requiring control room isolation, consideration that the remaining train can provide the required capabilities, and the alternate safety or nonsafety related cooling means that are available.

B.1 and B.2

In MODE 1, 2, 3, or 4, when Required Action A.1 cannot be completed within the required Completion Time, the unit must be placed in a MODE that minimizes the accident risk. To achieve this status, the unit must be placed in at least MODE 3 within 6 hours, and in MODE 5 within 36 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required unit conditions from full power conditions in an orderly manner and without challenging unit systems.

[C.1 and C.2

In MODE 5 or 6, or during movement of [recently] irradiated fuel assemblies, when Required Action A.1 cannot be completed within the required Completion Time, the OPERABLE CREATCS train must be placed in operation immediately. This action ensures that the remaining train is OPERABLE, that no failures preventing automatic actuation will occur, and that any active failure will be readily detected.

An alternative to Required Action C.1 is to immediately suspend activities that could result in a release of radioactivity that might require isolation of the control room. This places the unit in a condition that minimizes the accident risk. This does not preclude the movement of fuel assemblies to a safe position.]

BASES

ACTIONS (continued)

[D.1

In [MODE 5 or 6, or] during movement of [recently] irradiated fuel assemblies, with two CREATCS trains inoperable, action must be taken immediately to suspend activities that could result in a release of radioactivity that might require isolation of the control room. This places the unit in a condition that minimizes the accident risk. This does not preclude the movement of fuel to a safe position.]

E.1

If both CREATCS trains are inoperable in MODE 1, 2, 3, or 4, the CREATCS may not be capable of performing the intended function and the unit is in a condition outside the accident analysis. Therefore, LCO 3.0.3 must be entered immediately.

SURVEILLANCE REQUIREMENTS

SR 3.7.12.1

This SR verifies that the heat removal capability of the system is sufficient to meet design requirements. This SR consists of a combination of testing and calculations. An [18] month Frequency is appropriate, since significant degradation of the CREATCS is slow and is not expected over this time period.

REFERENCES

1. FSAR, Section [6.4].

B 3.7 PLANT SYSTEMS

B 3.7.13 Emergency Core Cooling System (ECCS) Pump Room Exhaust Air Cleanup System (PREACS)

BASES

BACKGROUND

The ECCS PREACS filters air from the area of the active ECCS components during the recirculation phase of a loss of coolant accident (LOCA). The ECCS PREACS, in conjunction with other, normally operating systems, also provides environmental control of temperature and humidity in the ECCS pump room area and the lower reaches of the Auxiliary Building.

The ECCS PREACS consists of two independent and redundant trains. Each train consists of a heater, a prefilter or demister, a high efficiency particulate air (HEPA) filter, an activated charcoal adsorber section for removal of gaseous activity (principally iodines), and a fan. Ductwork, valves or dampers, and instrumentation also form part of the system, as well as demisters functioning to reduce the relative humidity of the air stream. A second bank of HEPA filters follows the adsorber section to collect carbon fines and provide backup in case the main HEPA filter bank fails. The downstream HEPA filter is not credited in the accident analysis, but serves to collect charcoal fines and to back up the upstream HEPA filter, should it develop a leak. The system initiates filtered ventilation of the pump room and lower region of the Auxiliary Building following receipt of a safety injection actuation signal or coolant injection actuation signal.

The ECCS PREACS is a standby system, parts of which may also operate during normal unit operations. The Reactor Auxiliary Building Main Ventilation System provides normal cooling. During emergency operations, the ECCS PREACS dampers are realigned and fans are started to initiate filtration. Upon receipt of the actuating Engineered Safety Feature Actuation System signal(s), normal air discharges from the ECCS pump room, the pump room is isolated, and the stream of ventilation air discharges through the system filter trains. The prefilters or demisters remove any large particles in the air, and any entrained water droplets present, to prevent excessive loading of the HEPA filters and charcoal adsorbers.

The ECCS PREACS is discussed in the FSAR, Sections [6.5.1], [9.4.5], and [15.6.5] (Refs. 1, 2, and 3, respectively), as it may be used for normal, as well as post accident, atmospheric cleanup functions. The primary purpose of the heaters is to maintain the relative humidity at an acceptable level consistent with iodine removal efficiencies, as discussed in the Regulatory Guide 1.52 (Ref. 4).

BASES

APPLICABLE SAFETY ANALYSES

The design basis of the ECCS PREACS is established by the large break LOCA. The system evaluation assumes a passive failure of the ECCS outside containment, such as safety injection pump seal failure, during the recirculation mode. In such a case, the system limits the radioactive release to within 10 CFR 100 limits (Ref. 5), or the NRC staff approved licensing basis (e.g., a specified fraction of 10 CFR 100 limits). The analysis of the effects and consequences of a large break LOCA is presented in Reference 3. The ECCS PREACS also actuates following a small break LOCA, requiring the unit to go into the recirculation mode of long term cooling and to clean up releases of smaller leaks, such as from valve stem packing.

The two types of system failures that are considered in the accident analysis are complete loss of function and excessive LEAKAGE. Either type of failure may result in a lower efficiency of removal for any gaseous and particulate activity released to the ECCS pump rooms following a LOCA.

The ECCS PREACS satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

Two independent and redundant ECCS PREACS trains are required to be OPERABLE to ensure that at least one is available, assuming a single failure disables the other train coincident with a loss of offsite power. Total system failure could result in the atmospheric release from the ECCS pump room exceeding the required limits in the event of a Design Basis Accident (DBA).

ECCS PREACS is considered OPERABLE when the individual components necessary to maintain the ECCS Pump Room filtration are OPERABLE in both trains.

An ECCS PREACS train is considered OPERABLE when its associated:

a. Fan is OPERABLE,

b. HEPA filter and charcoal adsorber are not excessively restricting flow and are capable of performing their filtration functions, and

c. Heater, demister, ductwork, valves, and dampers are OPERABLE, and air circulation can be maintained.

BASES

LCO (continued)

The LCO is modified by a Note allowing the ECCS pump room boundary to be opened intermittently under administrative controls. For entry and exit through doors, the administrative control of the opening is performed by the person(s) entering or exiting the area. For other openings, these controls consist of stationing a dedicated individual at the opening who is in continuous communication with the control room. This individual will have a method to rapidly close the opening when a need for ECCS pump room isolation is indicated.

APPLICABILITY

In MODES 1, 2, 3, and 4, the ECCS PREACS is required to be OPERABLE consistent with the OPERABILITY requirements of the ECCS.

In MODES 5 and 6, the ECCS PREACS is not required to be OPERABLE, since the ECCS is not required to be OPERABLE.

ACTIONS

A.1

With one ECCS PREACS train inoperable, action must be taken to restore OPERABLE status within 7 days. During this time, the remaining OPERABLE train is adequate to perform the ECCS PREACS function.

The 7 day Completion Time is appropriate because the risk contribution is less than that for the ECCS (72 hour Completion Time) and this system is not a direct support system for the ECCS. The 7 day Completion Time is reasonable, based on the low probability of a DBA occurring during this time period, and the consideration that the remaining train can provide the required capability.

B.1

----------------------------------REVIEWER'S NOTE----------------------------------
Adoption of Condition B is dependent on a commitment from the licensee to have guidance available describing compensatory measures to be taken in the event of an intentional and unintentional entry into Condition B.

BASES

ACTIONS (continued)

If the ECCS pump room boundary is inoperable, the ECCS PREACS trains cannot perform their intended functions. Actions must be taken to restore an OPERABLE ECCS pump room boundary within 24 hours. During the period that the ECCS pump room boundary is inoperable, appropriate compensatory measures [consistent with the intent, as applicable, of GDC 19, 60, 64 and 10 CFR Part 100] should be utilized to protect plant personnel from potential hazards such as radioactive contamination, toxic chemicals, smoke, temperature and relative humidity, and physical security. Preplanned measures should be available to address these concerns for intentional and unintentional entry into the condition. The 24 hour Completion Time is reasonable based on the low probability of a DBA occurring during this time period, and the use of compensatory measures. The 24 hour Completion Time is a typically reasonable time to diagnose, plan and possibly repair, and test most problems with the ECCS pump room boundary.

C.1 and C.2

If the ECCS PREACS train or ECCS pump room boundary cannot be restored to OPERABLE status within the associated Completion Time, the unit must be in a MODE in which the LCO does not apply. To achieve this status, the unit must be placed in at least MODE 3 within 6 hours, and in MODE 5 within 36 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required unit conditions from full power conditions in an orderly manner and without challenging unit systems.

SURVEILLANCE REQUIREMENTS

SR 3.7.13.1

Standby systems should be checked periodically to ensure that they function properly. Since the environment and normal operating conditions on this system are not severe, testing each train once a month provides an adequate check on this system. Monthly heater operations dry out any moisture that may have accumulated in the charcoal from humidity in the ambient air. [Systems with heaters must be operated for ≥ 10 continuous hours with the heaters energized. Systems without heaters need only be operated for ≥ 15 minutes to demonstrate the function of the system.] The 31 day Frequency is based on the known reliability of equipment, and the two train redundancy available.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.7.13.2

This SR verifies that the required ECCS PREACS testing is performed in accordance with the [Ventilation Filter Testing Program (VFTP)]. The [VFTP] includes testing HEPA filter performance, charcoal adsorber efficiency, minimum system flow rate, and the physical properties of the activated charcoal (general use and following specific operations). Specific test frequencies and additional information are discussed in detail in the [VFTP].

SR 3.7.13.3

This SR verifies that each ECCS PREACS train starts and operates on an actual or simulated actuation signal. The [18] month Frequency is consistent with that specified in Regulatory Guide 1.52 (Ref. 4).

SR 3.7.13.4

This SR verifies the integrity of the ECCS pump room enclosure. The ability of the ECCS pump room to maintain a negative pressure, with respect to potentially uncontaminated adjacent areas, is periodically tested to verify proper function of the ECCS PREACS. During the post accident mode of operation, the ECCS PREACS is designed to maintain a slight negative pressure in the ECCS pump room with respect to adjacent areas to prevent unfiltered LEAKAGE. The ECCS PREACS is designed to maintain this negative pressure at a flow rate of ≤ [20,000] cfm from the ECCS pump room. The Frequency of [18] months is consistent with the guidance provided in the NUREG-0800, Section 6.5.1 (Ref. 6).

This test is conducted with the tests for filter penetration; thus, an [18] month Frequency, on a STAGGERED TEST BASIS is consistent with other filtration SRs.

[SR 3.7.13.5

Operating the ECCS PREACS filter bypass damper is necessary to ensure that the system functions properly. The OPERABILITY of the bypass damper is verified if it can be closed. An [18] month Frequency is consistent with that specified in Reference 4.]

BASES

REFERENCES

1. FSAR, Section [6.5.1].
2. FSAR, Section [9.4.5].
3. FSAR, Section [15.6.5].
4. Regulatory Guide 1.52, Rev. [2].
5. 10 CFR 100.11.
6. NUREG-0800, Section 6.5.1, Rev. 2, July 1981.

B 3.7 PLANT SYSTEMS

B 3.7.14 Fuel Building Air Cleanup System (FBACS)

BASES

BACKGROUND

The FBACS filters airborne radioactive particulates from the area of the fuel pool following a fuel handling accident or loss of coolant accident. The FBACS, in conjunction with other normally operating systems, also provides environmental control of temperature and humidity in the fuel pool area.

The FBACS consists of two independent, redundant trains. Each train consists of a heater, a prefilter or demister, a high efficiency particulate air (HEPA) filter, an activated charcoal adsorber section for removal of gaseous activity (principally iodines), and a fan. Ductwork, valves or dampers, and instrumentation also form part of the system, as well as demisters, functioning to reduce the relative humidity of the air stream. A second bank of HEPA filters follows the adsorber section to collect carbon fines and provide backup in case of failure of the main HEPA filter bank. The downstream HEPA filter is not credited in the analysis, but serves to collect charcoal fines, and to back up the upstream HEPA filter should it develop a leak. The system initiates filtered ventilation of the fuel handling building following receipt of a high radiation signal.

The FBACS is a standby system, part of which may also be operated during normal unit operations. Upon receipt of the actuating signal, normal air discharges from the fuel handling building, the fuel handling building is isolated, and the stream of ventilation air discharges through the system filter trains. The prefilters or demisters remove any large particles in the air, and any entrained water droplets present, to prevent excessive loading of the HEPA filters and charcoal adsorbers.

The FBACS is discussed in the FSAR, Sections [6.5.1], [9.4.5], and [15.7.4] (Refs. 1, 2, and 3, respectively), because it may be used for normal, as well as post accident, atmospheric cleanup functions.

APPLICABLE SAFETY ANALYSES

The FBACS is designed to mitigate the consequences of a fuel handling accident [involving handling recently irradiated fuel (i.e., fuel that has occupied part of a critical reactor core within the previous [X] days)] in which [all] rods in the fuel assembly are assumed to be damaged. The analysis of the fuel handling accident is given in Reference 3. The

BASES

APPLICABLE SAFETY ANALYSES (continued)

Design Basis Accident analysis of the fuel handling accident assumes that only one train of the FBACS is functional, due to a single failure that disables the other train. The accident analysis accounts for the reduction in airborne radioactive material provided by the remaining one train of this filtration system. The amount of fission products available for release from the fuel handling building is determined for a fuel handling accident. These assumptions and the analysis follow the guidance provided in Regulatory Guide 1.25 (Ref. 4).

The FBACS satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

Two independent and redundant trains of the FBACS are required to be OPERABLE to ensure that at least one is available, assuming a single failure that disables the other train coincident with a loss of offsite power. Total system failure could result in the atmospheric release from the fuel building exceeding the 10 CFR 100 limits (Ref. 5) in the event of a fuel handling accident.

The FBACS is considered OPERABLE when the individual components necessary to control exposure in the fuel handling building are OPERABLE in both trains. An FBACS train is considered OPERABLE when its associated:

a. Fan is OPERABLE,

b. HEPA filter and charcoal adsorber are not excessively restricting flow, and are capable of performing their filtration functions, and

c. Heater, demister, ductwork, valves, and dampers are OPERABLE, and air circulation can be maintained.

The LCO is modified by a Note allowing the fuel building boundary to be opened intermittently under administrative controls. For entry and exit through doors, the administrative control of the opening is performed by the person(s) entering and exiting the area. For other openings, these controls consist of stationing a dedicated individual at the opening who is in continuous communication with the control room. This individual will have a method to rapidly close the opening when a need for fuel building isolation is indicated.

BASES

APPLICABILITY

In MODES 1, 2, 3, and 4, the FBACS is required to be OPERABLE to provide fission product removal associated with ECCS leaks due to a LOCA (refer to LCO 3.7.13, "Emergency Core Cooling System (ECCS) Pump Room Exhaust Air Cleanup System (PREACS)") for units that use this system as part of their ECCS PREACS.

During movement of [recently] irradiated fuel assemblies in the fuel building, the FBACS is required to be OPERABLE to mitigate the consequences of a fuel handling accident [involving handling recently irradiated fuel. Due to radioactive decay, FBACS is only required to mitigate fuel handling accidents involving handling recently irradiated fuel (i.e., fuel that has occupied part of a critical reactor core within the previous [X] days)].

In MODES 5 and 6, the FBACS is not required to be OPERABLE, since the ECCS is not required to be OPERABLE.

ACTIONS

LCO 3.0.3 is not applicable while in MODE 5 or 6. However, since irradiated fuel assembly movement can occur in MODE 1, 2, 3, or 4, the ACTIONS have been modified by a Note stating that LCO 3.0.3 is not applicable. If moving irradiated fuel assemblies while in MODE 5 or 6, LCO 3.0.3 would not specify any action. If moving irradiated fuel assemblies while in MODE 1, 2, 3, or 4, the fuel movement is independent of reactor operations. Entering LCO 3.0.3, while in MODE 1, 2, 3, or 4 would require the unit to be shutdown unnecessarily.

A.1

If one FBACS train is inoperable, action must be taken to restore OPERABLE status within 7 days. During this time period, the remaining OPERABLE train is adequate to perform the FBACS function. The 7 day Completion Time is reasonable, based on the risk from an event occurring requiring the inoperable FBACS train, and ability of the remaining FBACS train to provide the required protection.

B.1

-----------------------------------REVIEWER'S NOTE-----------------------------------
Adoption of Condition B is dependent on a commitment from the licensee to have guidance available describing compensatory measures to be taken in the event of an intentional and unintentional entry into Condition B.

BASES

ACTIONS (continued)

If the fuel building boundary is inoperable in MODE 1, 2, 3, or 4, the FBACS trains cannot perform their intended functions. Actions must be taken to restore an OPERABLE fuel building boundary within 24 hours. During the period that the fuel building boundary is inoperable, appropriate compensatory measures [consistent with the intent, as applicable, of GDC 19, 60, 61, 63, 64 and 10 CFR Part 100] should be utilized to protect plant personnel from potential hazards such as radioactive contamination, toxic chemicals, smoke, temperature and relative humidity, and physical security. Preplanned measures should be available to address these concerns for intentional and unintentional entry into the condition. The 24 hour Completion Time is reasonable based on the low probability of a DBA occurring during this time period, and the use of compensatory measures. The 24 hour Completion Time is a typically reasonable time to diagnose, plan and possibility repair, and test most problems with the fuel building boundary.

[C.1 and C.2

In MODE 1, 2, 3, or 4, when Required Action A.1 or B.1 cannot be completed within the Completion Time, or when both FBACS trains are inoperable for reasons other than an inoperable fuel building boundary (i.e., Condition B), the unit must be placed in a MODE in which the LCO does not apply. To achieve this status, the unit must be placed in MODE 3 within 6 hours, and in MODE 5 within 36 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required unit conditions from full power conditions in an orderly manner and without challenging unit systems.]

D.1 and D.2

When Required Action A.1 cannot be completed within the required Completion Time during movement of [recently] irradiated fuel assemblies in the fuel building, the OPERABLE FBACS train must be started immediately or fuel movement suspended. This action ensures that the remaining train is OPERABLE, that no undetected failures preventing system operation will occur, and that any active failure will be readily detected.

If the system is not placed in operation, this action requires suspension of [recently] irradiated fuel movement, which precludes a fuel handling accident. This does not preclude the movement of fuel to a safe position.

BASES

ACTIONS (continued)

E.1

When two trains of the FBACS are inoperable during movement of [recently] irradiated fuel assemblies in the fuel building, action must be taken to place the unit in a condition in which the LCO does not apply. This LCO involves immediately suspending movement of [recently] irradiated fuel assemblies in the fuel building. This does not preclude the movement of fuel to a safe position.

SURVEILLANCE REQUIREMENTS

SR 3.7.14.1

Standby systems should be checked periodically to ensure that they function properly. As the environment and normal operating conditions on this system are not severe, testing each train once every month provides an adequate check on this system. Monthly heater operation dries out any moisture accumulated in the charcoal from humidity in the ambient air. [Systems with heaters must be operated for ≥ 10 continuous hours with the heaters energized. Systems without heaters need only be operated for ≥ 15 minutes to demonstrate the function of the system.] The 31 day Frequency is based on the known reliability of the equipment and the two train redundancy available.

SR 3.7.14.2

This SR verifies the performance of FBACS filter testing in accordance with the [Ventilation Filter Testing Program (VFTP)]. The [VFTP] includes testing HEPA filter performance, charcoal adsorber efficiency, minimum system flow rate, and the physical properties of the activated charcoal (general use and following specific operations). Specific test frequencies and additional information are discussed in detail in the [VFTP].

[SR 3.7.14.3

This SR verifies that each FBACS train starts and operates on an actual or simulated actuation signal. The [18] month Frequency is consistent with that specified in Reference 6.]

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.7.14.4

This SR verifies the integrity of the fuel building enclosure. The ability of the fuel building to maintain negative pressure with respect to potentially uncontaminated adjacent areas is periodically tested to verify proper function of the FBACS. During the post accident mode of operation, the FBACS is designed to maintain a slight negative pressure in the fuel building, with respect to adjacent areas, to prevent unfiltered LEAKAGE. The FBACS is designed to maintain this negative pressure at a flow rate of ≤ [3000] cfm to the fuel building. The Frequency of [18] months is consistent with the guidance provided in NUREG-0800, Section 6.5.1 (Ref. 7).

This test is conducted with the tests for filter penetration; thus, an [18] month Frequency, on a STAGGERED TEST BASIS is consistent with other filtration SRs.

[SR 3.7.14.5

Operating the FBACS filter bypass damper is necessary to ensure that the system functions properly. The OPERABILITY of the FBACS filter bypass damper is verified if it can be closed. The 18 month Frequency is consistent with that specified in Reference 6.]

REFERENCES

1. FSAR, Section [6.5.1].
2. FSAR, Section [9.4.5].
3. FSAR, Section [15.7.4].
4. Regulatory Guide 1.25.
5. 10 CFR 100.
6. Regulatory Guide 1.52, Rev. [2].
7. NUREG-0800, Section 6.5.1, July 1981.

B 3.7 PLANT SYSTEMS

B 3.7.15 Penetration Room Exhaust Air Cleanup System (PREACS)

BASES

BACKGROUND

The PREACS filters air from the penetration area between containment and the Auxiliary Building.

The PREACS consists of two independent and redundant trains. Each train consists of a heater, a prefilter or demister, a high efficiency particulate air (HEPA) filter, an activated charcoal adsorber section for removal of gaseous activity (principally iodines), and a fan. Ductwork, valves or dampers, and instrumentation also form part of the system, as well as demisters functioning to reduce the relative humidity of the air stream. A second bank of HEPA filters, which follows the adsorber section, collects carbon fines and provides backup in case of failure of the main HEPA filter bank. The downstream HEPA filter, although not credited in the accident analysis, collects charcoal fines and serves as a backup should the upstream HEPA filter develop a leak. The system initiates filtered ventilation following receipt of a safety injection actuation signal or containment isolation actuation signal.

The PREACS is a standby system, parts of which may also operate during normal unit operations. During emergency operations, the PREACS dampers are realigned, and fans are started to initiate filtration. Upon receipt of the actuating Engineered Safety Feature Actuation System signal(s), normal air discharges from the penetration room, the penetration room is isolated, and the stream of ventilation air discharges through the system filter trains. The prefilters or demisters remove any large particles in the air, as well as any entrained water droplets, to prevent excessive loading of the HEPA filters and charcoal adsorbers.

The PREACS is discussed in the FSAR, Sections [6.5.1], [9.4.5], and [15.6.5] (Refs. 1, 2, and 3, respectively), as it may be used for normal, as well as post accident, atmospheric cleanup functions. Heaters may be included for moisture removal on systems operating in high humidity conditions. The primary purpose of the heaters is to maintain the relative humidity at an acceptable level, consistent with iodine removal efficiencies, as discussed in the Regulatory Guide 1.52 (Ref. 4).

BASES

APPLICABLE SAFETY ANALYSES	The design basis of the PREACS is established by the large break loss of coolant accident (LOCA). The system evaluation assumes a passive failure outside containment, such as a valve packing leakage during a Design Basis Accident (DBA). In such a case, the system restricts the radioactive release to within 10 CFR 100 (Ref. 5) limits, or the NRC staff approved licensing basis (e.g., a specified fraction of 10 CFR 100 limits). The analysis of the effects and consequences of a large break LOCA are presented in Reference 3. There are two types of system failures considered in the accident analysis: a complete loss of function and an excessive LEAKAGE. Either type of failure may result in less efficient removal for any gaseous or particulate material released to the penetration rooms following a LOCA. The PREACS satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).
LCO	Two independent and redundant trains of the PREACS are required to be OPERABLE to ensure that at least one train is available, assuming there is a single failure disabling the other train coincident with a loss of offsite power. The PREACS is considered OPERABLE when the individual components necessary to control radioactive releases are OPERABLE in both trains. A PREACS train is considered OPERABLE when its associated: a. Fan is OPERABLE, b. HEPA filter and charcoal absorber are not excessively restricting flow, and are capable of performing the filtration functions, and c. Heater, demister, ductwork, valves, and dampers are OPERABLE, and circulation can be maintained. The LCO is modified by a Note allowing the penetration room boundary to be opened intermittently under administrative controls. For entry and exit through doors, the administrative control of the opening is performed by the person(s) entering or exiting the area. For other openings, these controls consist of stationing a dedicated individual at the opening who is in continuous communication with the control room. This individual will have a method to rapidly close the opening when a need for penetration room isolation is indicated.
APPLICABILITY	In MODES 1, 2, 3, and 4, the PREACS is required to be OPERABLE, consistent with the OPERABILITY requirements of the Emergency Core Cooling System (ECCS). In MODES 5 and 6, the PREACS is not required to be OPERABLE, since the ECCS is not required to be OPERABLE.

BASES

ACTIONS

A.1

With one PREACS train inoperable, action must be taken to restore OPERABLE status within 7 days. During this time period, the remaining OPERABLE train is adequate to perform the PREACS function. The 7 day Completion Time is appropriate because the risk contribution of the PREACS is less than that for the ECCS (72 hour Completion Time), and because this system is not a direct support system for the ECCS. The 7 day Completion Time is reasonable based on the low probability of a DBA occurring during this time period, and the consideration that the remaining train can provide the required capability.

B.1

-----------------------------------REVIEWER'S NOTE-----------------------------------
Adoption of Condition B is dependent on a commitment from the licensee to have guidance available describing compensatory measures to be taken in the event of an intentional and unintentional entry into Condition B.

If the penetration room boundary is inoperable, the PREACS trains cannot perform their intended functions. Actions must be taken to restore an OPERABLE penetration room boundary within 24 hours. During the period that the penetration room boundary is inoperable, appropriate compensatory measures [consistent with the intent, as applicable, of GDC 19, 60, 64 and 10 CFR Part 100] should be utilized to protect plant personnel from potential hazards such as radioactive contamination, toxic chemicals, smoke, temperature and relative humidity, and physical security. Preplanned measures should be available to address these concerns for intentional and unintentional entry into the condition. The 24 hour Completion Time is reasonable based on the low probability of a DBA occurring during this time period, and the use of compensatory measures. The 24 hour Completion Time is reasonable based on the low probability of a DBA occurring during this time period, and the use of compensatory measures. The 24 hour Completion Time is a typically reasonable time to diagnose, plan and possibly repair, and test most problems with the penetration room boundary.

BASES

ACTIONS (continued)

C.1 and C.2

If the inoperable PREACS train or penetration room boundary cannot be restored to OPERABLE status within the associated Completion Time, the unit must be placed in a MODE in which the LCO does not apply. To achieve this status, the unit must be placed in at least MODE 3 within 6 hours, and in MODE 5 within 36 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required unit conditions from full power conditions in an orderly manner and without challenging unit systems.

SURVEILLANCE REQUIREMENTS

SR 3.7.15.1

Standby systems should be checked periodically to ensure that they function properly. As the environment and normal operating conditions on this system are not severe, testing each train once every month provides an adequate check on this system.

Monthly heater operation dries out any moisture that may have accumulated in the charcoal as a result of humidity in the ambient air. [Systems with heaters must be operated for ≥ 10 continuous hours with the heaters energized. Systems without heaters need only be operated for ≥ 15 minutes to demonstrate the function of the system.] The 31 day Frequency is based on the known reliability of the equipment and the two train redundancy available.

SR 3.7.15.2

This SR verifies the performance of PREACS filter testing in accordance with the [Ventilation Filter Testing Program (VFTP)]. The [VFTP] includes testing the performance of the HEPA filter, charcoal adsorber efficiency, minimum system flow rate, and the physical properties of the activated charcoal (general use and following specific operations). Specific test frequencies and additional information are discussed in detail in the [VFTP].

[SR 3.7.15.3

This SR verifies that each PREACS train starts and operates on an actual or simulated actuation signal. The [18] month Frequency is consistent with that specified in Reference 4.]

BASES

SURVEILLANCE REQUIREMENTS (continued)

[SR 3.7.15.4

This SR verifies the integrity of the penetration room enclosure. The ability of the penetration room to maintain negative pressure, with respect to potentially uncontaminated adjacent areas, is periodically tested to verify proper function of the PREACS. During the post accident mode of operation, PREACS is designed to maintain a slightly negative pressure at a flow rate of ≤ [3000] cfm in the penetration room with respect to adjacent areas to prevent unfiltered LEAKAGE. The Frequency of [18] months is consistent with the guidance provided in NUREG-0800, Section 6.5.1 (Ref. 6).]

[The minimum system flow rate maintains a slight negative pressure in the penetration room area and provides sufficient air velocity to transport particulate contaminants, assuming only one filter train is operating.

The number of filter elements is selected to limit the flow rate through any individual element to about [1000] cfm. This may vary based on filter housing geometry. The maximum limit ensures that flow through, and pressure drop across, each filter element is not excessive.

The number and depth of the adsorber elements ensures that, at the maximum flow rate, the residence time of the air stream in the charcoal bed achieves the desired adsorption rate. At least a [0.125] second residence time is necessary for an assumed [99]% efficiency.

The filters have a certain pressure drop at the design flow rate when clean. The magnitude of the pressure drop indicates acceptable performance, and is based on manufacturer's recommendations for the filter and adsorber elements at the design flow rate. An increase in pressure drop or decrease in flow indicates that the filter is being loaded or is indicative of other problems with the system.

This test is conducted with the tests for filter penetration; thus, an [18] month Frequency on a STAGGERED TEST BASIS consistent with other filtration SRs.]

[SR 3.7.15.5

Operating the PREACS filter bypass damper is necessary to ensure that the system functions properly. The OPERABILITY of the PREACS filter bypass damper is verified if it can be closed. An [18] month Frequency is consistent with that specified in Reference 4.]

BASES

REFERENCES

1. FSAR, Section [6.5.1].
2. FSAR, Section [9.4.5].
3. FSAR, Section [15.6.5].
4. Regulatory Guide 1.52 Rev. [2].
5. 10 CFR 100.11.
6. NUREG-0800, Section 6.5.1.

B 3.7 PLANT SYSTEMS

B 3.7.16 Fuel Storage Pool Water Level

BASES

BACKGROUND	The minimum water level in the fuel storage pool meets the assumptions of iodine decontamination factors following a fuel handling accident. The specified water level shields and minimizes the general area dose when the storage racks are filled to their maximum capacity. The water also provides shielding during the movement of spent fuel. A general description of the fuel storage pool design is given in the FSAR, Section [9.1.2], Reference 1, and the Spent Fuel Pool Cooling and Cleanup System is given in the FSAR, Section [9.1.3] (Ref. 2). The assumptions of the fuel handling accident are given in the FSAR, Section [15.7.4] (Ref. 3).
APPLICABLE SAFETY ANALYSES	The minimum water level in the fuel storage pool meets the assumptions of the fuel handling accident described in Regulatory Guide 1.25 (Ref. 4). The resultant 2 hour thyroid dose to a person at the exclusion area boundary is a small fraction of the 10 CFR 100 (Ref. 5) limits. According to Reference 4, there is 23 ft of water between the top of the damaged fuel bundle and the fuel pool surface for a fuel handling accident. With a 23 ft water level, the assumptions of Reference 4 can be used directly. In practice, this LCO preserves this assumption for the bulk of the fuel in the storage racks. In the case of a single bundle, dropped and lying horizontally on top of the spent fuel racks, however, there may be < 23 ft of water above the top of the bundle and the surface, by the width of the bundle. To offset this small nonconservatism, the analysis assumes that all fuel rods fail, although analysis shows that only the first few rods fail from a hypothetical maximum drop. The fuel storage pool water level satisfies Criteria 2 and 3 of 10 CFR 50.36(c)(2)(ii).
LCO	The specified water level preserves the assumptions of the fuel handling accident analysis (Ref. 3). As such, it is the minimum required for fuel storage and movement within the fuel storage pool.
APPLICABILITY	This LCO applies during movement of irradiated fuel assemblies in the fuel storage pool since the potential for a release of fission products exists.

BASES

ACTIONS

A.1

Required Action A.1 is modified by a Note indicating that LCO 3.0.3 does not apply.

When the initial conditions for an accident cannot be met, steps should be taken to preclude the accident from occurring. When the fuel storage pool water level is lower than the required level, the movement of irradiated fuel assemblies in the fuel storage pool is immediately suspended. This effectively precludes a spent fuel handling accident from occurring. This does not preclude moving a fuel assembly to a safe position.

If moving irradiated fuel assemblies while in MODE 5 or 6, LCO 3.0.3 would not specify any action. If moving irradiated fuel assemblies while in MODES 1, 2, 3, and 4, the fuel movement is independent of reactor operations. Therefore, in either case, inability to suspend movement of irradiated fuel assemblies is not sufficient reason to require a reactor shutdown.

SURVEILLANCE REQUIREMENTS

SR 3.7.16.1

This SR verifies sufficient fuel storage pool water is available in the event of a fuel handling accident. The water level in the fuel storage pool must be checked periodically. The 7 day Frequency is appropriate because the volume in the pool is normally stable. Water level changes are controlled by unit procedures and are acceptable, based on operating experience.

During refueling operations, the level in the fuel storage pool is at equilibrium with that of the refueling canal, and the level in the refueling canal is checked daily in accordance with LCO 3.7.17, "Fuel Storage Pool Boron Concentration."

REFERENCES

1. FSAR, Section [9.1.2].

2. FSAR, Section [9.1.3].

3. FSAR, Section [15.7.4].

4. Regulatory Guide 1.25.

5. 10 CFR 100.11.

B 3.7 PLANT SYSTEMS

B 3.7.17 Fuel Storage Pool Boron Concentration

BASES

BACKGROUND	As described in LCO 3.7.18, "Spent Fuel Assembly Storage," fuel assemblies are stored in the spent fuel racks [in a "checkerboard" pattern] in accordance with criteria based on [initial enrichment and discharge burnup]. Although the water in the spent fuel pool is normally borated to ≥ [1800] ppm, the criteria that limit the storage of a fuel assembly to specific rack locations is conservatively developed without taking credit for boron.
APPLICABLE SAFETY ANALYSES	A fuel assembly could be inadvertently loaded into a spent fuel rack location not allowed by LCO 3.7.18 (e.g., an unirradiated fuel assembly or an insufficiently depleted fuel assembly). This accident is analyzed assuming the extreme case of completely loading the fuel pool racks with unirradiated assemblies of maximum enrichment. Another type of postulated accident is associated with a fuel assembly that is dropped onto the fully loaded fuel pool storage rack. Either incident could have a positive reactivity effect, decreasing the margin to criticality. However, the negative reactivity effect of the soluble boron compensates for the increased reactivity caused by either one of the two postulated accident scenarios. The concentration of dissolved boron in the fuel pool satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).
LCO	The specified concentration of dissolved boron in the fuel pool preserves the assumptions used in the analyses of the potential accident scenarios described above. This concentration of dissolved boron is the minimum required concentration for fuel assembly storage and movement within the fuel pool.
APPLICABILITY	This LCO applies whenever fuel assemblies are stored in the spent fuel pool until a complete spent fuel pool verification has been performed following the last movement of fuel assemblies in the spent fuel pool. This LCO does not apply following the verification since the verification would confirm that there are no misloaded fuel assemblies. With no further fuel assembly movements in progress, there is no potential for a misloaded fuel assembly or a dropped fuel assembly.

BASES

ACTIONS

A.1, A.2.1, and A.2.2

The Required Actions are modified by a Note indicating that LCO 3.0.3 does not apply.

When the concentration of boron in the spent fuel pool is less than required, immediate action must be taken to preclude an accident from happening or to mitigate the consequences of an accident in progress. This is most efficiently achieved by immediately suspending the movement of fuel assemblies. This does not preclude the movement of fuel assemblies to a safe position. In addition, action must be immediately initiated to restore boron concentration to within limit. Alternately, beginning a verification of the fuel storage pool fuel locations, to ensure proper locations of the fuel, can be performed.

If moving irradiated fuel assemblies while in MODE 5 or 6, LCO 3.0.3 would not specify any action. If moving irradiated fuel assemblies while in MODE 1, 2, 3, or 4, the fuel movement is independent of reactor operation. Therefore, inability to suspend movement of fuel assemblies is not sufficient reason to require a reactor shutdown.

SURVEILLANCE REQUIREMENTS

SR 3.7.17.1

This SR verifies that the concentration of boron in the spent fuel pool is within the required limit. As long as this SR is met, the analyzed incidents are fully addressed. The 7 day Frequency is appropriate because no major replenishment of pool water is expected to take place over a short period of time.

REFERENCES

None.

B 3.7 PLANT SYSTEMS

B 3.7.18 Spent Fuel Pool Storage

BASES

BACKGROUND	The spent fuel storage facility is designed to store either new (nonirradiated) nuclear fuel assemblies, or burned (irradiated) fuel assemblies in a vertical configuration underwater. The storage pool is sized to store [735] fuel assemblies, which includes storage for [15] failed fuel containers. The spent fuel storage cells are installed in parallel rows with center to center spacing of [12 31/32] inches in one direction, and [13 3/16] inches in the other orthogonal direction. This spacing and "flux trap" construction, whereby the fuel assemblies are inserted into neutron absorbing stainless steel cans, is sufficient to maintain a k_{eff} of ≤ 0.95 for spent fuel of original enrichment of up to [3.3]%. However, as higher initial enrichment fuel assemblies are stored in the spent fuel pool, they must be stored in a checkerboard pattern taking into account fuel burnup to maintain a k_{eff} of 0.95 or less.
APPLICABLE SAFETY ANALYSES	The spent fuel storage facility is designed for noncriticality by use of adequate spacing, and "flux trap" construction whereby the fuel assemblies are inserted into neutron absorbing stainless steel cans. The spent fuel pool storage satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).
LCO	The restrictions on the placement of fuel assemblies within the spent fuel pool, according to [Figure 3.7.18-1], in the accompanying LCO, ensures that the k_{eff} of the spent fuel pool will always remain < 0.95 assuming the pool to be flooded with unborated water. The restrictions are consistent with the criticality safety analysis performed for the spent fuel pool according to [Figure 3.7.18-1], in the accompanying LCO. Fuel assemblies not meeting the criteria of [Figure 3.7.18-1] shall be stored in accordance with Specification 4.3.1.1.
APPLICABILITY	This LCO applies whenever any fuel assembly is stored in [Region 2] of the spent fuel pool.
ACTIONS	<u>A.1</u> Required Action A.1 is modified by a Note indicating that LCO 3.0.3 does not apply. When the configuration of fuel assemblies stored in [Region 2] the spent fuel pool is not in accordance with Figure [3.7.18-1], immediate action must be taken to make the necessary fuel assembly movement(s) to bring the configuration into compliance with Figure [3.7.18-1].

BASES

ACTIONS (continued)

If moving irradiated fuel assemblies while in MODE 5 or 6, LCO 3.0.3 would not specify any action. If moving irradiated fuel assemblies while in MODE 1, 2, 3, or 4, the fuel movement is independent of reactor operation. Therefore, in either case, inability to move fuel assemblies is not sufficient reason to require a reactor shutdown.

SURVEILLANCE REQUIREMENTS

SR 3.7.18.1

This SR verifies by administrative means that the initial enrichment and burnup of the fuel assembly is in accordance with Figure [3.7.18-1] in the accompanying LCO. For fuel assemblies in the unacceptable range of [Figure 3.7.18-1], performance of this SR will ensure compliance with Specification 4.3.1.1.

REFERENCES

None.

B 3.7 PLANT SYSTEMS

B 3.7.19 Secondary Specific Activity

BASES

BACKGROUND

Activity in the secondary coolant results from steam generator tube outleakage from the Reactor Coolant System (RCS). Under steady state conditions, the activity is primarily iodines with relatively short half lives, and thus is indication of current conditions. During transients, I-131 spikes have been observed as well as increased releases of some noble gases. Other fission product isotopes, as well as activated corrosion products in lesser amounts, may also be found in the secondary coolant.

A limit on secondary coolant specific activity during power operation minimizes releases to the environment because of normal operation, anticipated operational occurrences, and accidents.

This limit is lower than the activity value that might be expected from a 1 gpm tube leak (LCO 3.4.13, "RCS Operational LEAKAGE") of primary coolant at the limit of 1.0 μCi/gm (LCO 3.4.16, "RCS Specific Activity"). The steam line failure is assumed to result in the release of the noble gas and iodine activity contained in the steam generator inventory, the feedwater, and reactor coolant LEAKAGE. Most of the isotopes have short half-lives (i.e., < 20 hours).

With the specified activity level, the resultant 2 hour thyroid dose to a person at the exclusion area boundary (EAB) would be about [.13] rem should the main steam safety valves (MSSVs) open for the 2 hours following a trip from full power.

Operating a unit at the allowable limits could result in a 2 hour EAB exposure of a small fraction of the 10 CFR 100 (Ref. 1) limits.

APPLICABLE SAFETY ANALYSES

The accident analysis of the main steam line break (MSLB), as discussed in the FSAR, Chapter [15] (Ref. 2), assumes the initial secondary coolant specific activity to have a radioactive isotope concentration of [0.10] μCi/gm DOSE EQUIVALENT I-131. This assumption is used in the analysis for determining the radiological consequences of the postulated accident. The accident analysis, based on this and other assumptions, shows that the radiological consequences of an MSLB do not exceed a small fraction of the unit EAB limits (Ref. 1) for whole body and thyroid dose rates.

BASES

APPLICABLE SAFETY ANALYSES (continued)

With the loss of offsite power, the remaining steam generator is available for core decay heat dissipation by venting steam to the atmosphere through MSSVs and atmospheric dump valves (ADVs). The Auxiliary Feedwater System supplies the necessary makeup to the steam generator. Venting continues until the reactor coolant temperature and pressure have decreased sufficiently for the Shutdown Cooling System to complete the cooldown.

In the evaluation of the radiological consequences of this accident, the activity released from the steam generator connected to the failed steam line is assumed to be released directly to the environment. The unaffected steam generator is assumed to discharge steam and any entrained activity through MSSVs and ADVs during the event.

Secondary specific activity limits satisfy Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

As indicated in the Applicable Safety Analyses, the specific activity limit in the secondary coolant system of ≤ [0.10] μCi/gm DOSE EQUIVALENT I-131 to limit the radiological consequences of a Design Basis Accident (DBA) to a small fraction of the required limit (Ref. 1).

Monitoring the specific activity of the secondary coolant ensures that when secondary specific activity limits are exceeded, appropriate actions are taken in a timely manner to place the unit in an operational MODE that would minimize the radiological consequences of a DBA.

APPLICABILITY

In MODES 1, 2, 3, and 4, the limits on secondary specific activity apply due to the potential for secondary steam releases to the atmosphere.

In MODES 5 and 6, the steam generators are not being used for heat removal. Both the RCS and steam generators are depressurized, and primary to secondary LEAKAGE is minimal. Therefore, monitoring of secondary specific activity is not required.

BASES

ACTIONS	A.1 and A.2 DOSE EQUIVALENT I-131 exceeding the allowable value in the secondary coolant, is an indication of a problem in the RCS, and contributes to increased post accident doses. If secondary specific activity cannot be restored to within limits in the associated Completion Time, the unit must be placed in a MODE in which the LCO does not apply. To achieve this status, the unit must be placed in at least MODE 3 within 6 hours, and in MODE 5 within 36 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required unit conditions from full power conditions in an orderly manner and without challenging unit systems.
SURVEILLANCE REQUIREMENTS	SR 3.7.19.1 This SR ensures that the secondary specific activity is within the limits of the accident analysis. A gamma isotope analysis of the secondary coolant, which determines DOSE EQUIVALENT I-131, confirms the validity of the safety analysis assumptions as to the source terms in post accident releases. It also serves to identify and trend any unusual isotopic concentrations that might indicate changes in reactor coolant activity or LEAKAGE. The [31] day Frequency is based on the detection of increasing trends of the level of DOSE EQUIVALENT I-131, and allows for appropriate action to be taken to maintain levels below the LCO limit.
REFERENCES	1. 10 CFR 100.11. 2. FSAR, Chapter [15].

B 3.8 ELECTRICAL POWER SYSTEMS

B 3.8.1 AC Sources - Operating

BASES

BACKGROUND

The unit Class 1E Electrical Power Distribution System AC sources consist of the offsite power sources (preferred power sources, normal and alternate(s)), and the onsite standby power sources (Train A and Train B diesel generators (DGs)). As required by 10 CFR 50, Appendix A, GDC 17 (Ref. 1), the design of the AC electrical power system provides independence and redundancy to ensure an available source of power to the Engineered Safety Feature (ESF) systems.

The onsite Class 1E AC Distribution System is divided into redundant load groups (trains) so that the loss of any one group does not prevent the minimum safety functions from being performed. Each train has connections to two preferred offsite power sources and a single DG.

Offsite power is supplied to the unit switchyard(s) from the transmission network by [two] transmission lines. From the switchyard(s), two electrically and physically separated circuits provide AC power, through [step down station auxiliary transformers], to the 4.16 kV ESF buses. A detailed description of the offsite power network and the circuits to the Class 1E ESF buses is found in the FSAR, Chapter [8] (Ref. 2).

An offsite circuit consists of all breakers, transformers, switches, interrupting devices, cabling, and controls required to transmit power from the offsite transmission network to the onsite Class 1E ESF bus or buses.

Certain required unit loads are returned to service in a predetermined sequence in order to prevent overloading the transformer supplying offsite power to the onsite Class 1E Distribution System. Within [1 minute] after the initiating signal is received, all automatic and permanently connected loads needed to recover the unit or maintain it in a safe condition are returned to service via the load sequencer.

The onsite standby power source for each 4.16 kV ESF bus is a dedicated DG. DGs [11] and [12] are dedicated to ESF buses [11] and [12], respectively. A DG starts automatically on a safety injection (SI) signal (i.e., low pressurizer pressure or high containment pressure signals) or on an [ESF bus degraded voltage or undervoltage signal]. After the DG has started, it will automatically tie to its respective bus after offsite power is tripped as a consequence of ESF bus undervoltage or

BASES

BACKGROUND (continued)

degraded voltage, independent of or coincident with an SI signal. The DGs will also start and operate in the standby mode without tying to the ESF bus on an SI signal alone. Following the trip of offsite power, [a sequencer/an undervoltage signal] strips nonpermanent loads from the ESF bus. When the DG is tied to the ESF bus, loads are then sequentially connected to its respective ESF bus by the automatic load sequencer. The sequencing logic controls the permissive and starting signals to motor breakers to prevent overloading the DG by automatic load application.

In the event of a loss of preferred power, the ESF electrical loads are automatically connected to the DGs in sufficient time to provide for safe reactor shutdown and to mitigate the consequences of a Design Basis Accident (DBA) such as a loss of coolant accident (LOCA).

Certain required unit loads are returned to service in a predetermined sequence in order to prevent overloading the DG in the process. Within [1] minute after the initiating signal is received, all loads needed to recover the unit or maintain it in a safe condition are returned to service.

Ratings for Train A and Train B DGs satisfy the requirements of Regulatory Guide 1.9 (Ref. 3). The continuous service rating of each DG is [7000] kW with [10]% overload permissible for up to 2 hours in any 24 hour period. The ESF loads that are powered from the 4.16 kV ESF buses are listed in Reference 2.

APPLICABLE SAFETY ANALYSES

The initial conditions of DBA and transient analyses in the FSAR, Chapter [6] (Ref. 4) and Chapter [15] (Ref. 5), assume ESF systems are OPERABLE. The AC electrical power sources are designed to provide sufficient capacity, capability, redundancy, and reliability to ensure the availability of necessary power to ESF systems so that the fuel, Reactor Coolant System (RCS), and containment design limits are not exceeded. These limits are discussed in more detail in the Bases for Section 3.2, Power Distribution Limits; Section 3.4, Reactor Coolant System (RCS); and Section 3.6, Containment Systems.

The OPERABILITY of the AC electrical power sources is consistent with the initial assumptions of the accident analyses and is based upon meeting the design basis of the unit. This results in maintaining at least one train of the onsite or offsite AC sources OPERABLE during accident conditions in the event of:

BASES

APPLICABLE SAFETY ANALYSES (continued)

a. An assumed loss of all offsite power or all onsite AC power and

b. A worst case single failure.

The AC sources satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

Two qualified circuits between the offsite transmission network and the onsite Class 1E Electrical Power Distribution System and separate and independent DGs for each train ensure availability of the required power to shut down the reactor and maintain it in a safe shutdown condition after an anticipated operational occurrence (AOO) or a postulated DBA.

Qualified offsite circuits are those that are described in the FSAR and are part of the licensing basis for the unit.

[In addition, one required automatic load sequencer per train must be OPERABLE.]

Each offsite circuit must be capable of maintaining rated frequency and voltage, and accepting required loads during an accident, while connected to the ESF buses.

[Offsite circuit #1 consists of Safeguards Transformer B, which is supplied from Switchyard Bus B, and is fed through breaker 52-3 powering the ESF transformer XNB01, which, in turn, powers the #1 ESF bus through its normal feeder breaker. Offsite circuit #2 consists of the Startup Transformer, which is normally fed from the Switchyard Bus A, and is fed through breaker PA 0201 powering the ESF transformer, which, in turn, powers the #2 ESF bus through its normal feeder breaker.]

Each DG must be capable of starting, accelerating to rated speed and voltage, and connecting to its respective ESF bus on detection of bus undervoltage. This will be accomplished within [10] seconds. Each DG must also be capable of accepting required loads within the assumed loading sequence intervals, and continue to operate until offsite power can be restored to the ESF buses. These capabilities are required to be met from a variety of initial conditions such as DG in standby with the engine hot and DG in standby with the engine at ambient conditions. Additional DG capabilities must be demonstrated to meet required Surveillances, e.g., capability of the DG to revert to standby status on an ECCS signal while operating in parallel test mode.

BASES

LCO (continued)

Proper sequencing of loads, [including tripping of nonessential loads,] is a required function for DG OPERABILITY.

The AC sources in one train must be separate and independent (to the extent possible) of the AC sources in the other train. For the DGs, separation and independence are complete.

For the offsite AC sources, separation and independence are to the extent practical. A circuit may be connected to more than one ESF bus, with fast transfer capability to the other circuit OPERABLE, and not violate separation criteria. A circuit that is not connected to an ESF bus is required to have OPERABLE fast transfer interlock mechanisms to at least two ESF buses to support OPERABILITY of that circuit.

APPLICABILITY

The AC sources [and sequencers] are required to be OPERABLE in MODES 1, 2, 3, and 4 to ensure that:

a. Acceptable fuel design limits and reactor coolant pressure boundary limits are not exceeded as a result of AOOs or abnormal transients and

b. Adequate core cooling is provided and containment OPERABILITY and other vital functions are maintained in the event of a postulated DBA.

The AC power requirements for MODES 5 and 6 are covered in LCO 3.8.2, "AC Sources - Shutdown."

ACTIONS

A Note prohibits the application of LCO 3.0.4.b to an inoperable DG. There is an increased risk associated with entering a MODE or other specified condition in the Applicability with an inoperable DG and the provisions of LCO 3.0.4.b, which allow entry into a MODE or other specified condition in the Applicability with the LCO not met after performance of a risk assessment addressing inoperable systems and components, should not be applied in this circumstance.

A.1

To ensure a highly reliable power source remains with the one offsite circuit inoperable, it is necessary to verify the OPERABILITY of the remaining required offsite circuit on a more frequent basis. Since the Required Action only specifies "perform," a failure of SR 3.8.1.1 acceptance criteria does not result in a Required Action not met. However, if a second required circuit fails SR 3.8.1.1, the second offsite circuit is inoperable, and Condition C, for two offsite circuits inoperable, is entered.

BASES

ACTIONS (continued)

----------------------------------REVIEWER'S NOTE-----------------------------------

The turbine driven auxiliary feedwater pump is only required to be considered a redundant required feature, and, therefore, required to be determined OPERABLE by this Required Action, if the design is such that the remaining OPERABLE motor or turbine driven auxiliary feedwater pump(s) is not by itself capable (without any reliance on the motor driven auxiliary feedwater pump powered by the emergency bus associated with the inoperable diesel generator) of providing 100% of the auxiliary feedwater flow assumed in the safety analysis.

A.2

Required Action A.2, which only applies if the train cannot be powered from an offsite source, is intended to provide assurance that an event coincident with a single failure of the associated DG will not result in a complete loss of safety function of critical redundant required features. These features are powered from the redundant AC electrical power train. This includes motor driven auxiliary feedwater pumps. Single train systems, such as turbine driven auxiliary feedwater pumps, may not be included.

The Completion Time for Required Action A.2 is intended to allow the operator time to evaluate and repair any discovered inoperabilities. This Completion Time also allows for an exception to the normal "time zero" for beginning the allowed outage time "clock." In this Required Action, the Completion Time only begins on discovery that both:

a. The train has no offsite power supplying its loads and

b. A required feature on the other train is inoperable.

If at any time during the existence of Condition A (one offsite circuit inoperable) a redundant required feature subsequently becomes inoperable, this Completion Time begins to be tracked.

BASES

ACTIONS (continued)

Discovering no offsite power to one train of the onsite Class 1E Electrical Power Distribution System coincident with one or more inoperable required support or supported features, or both, that are associated with the other train that has offsite power, results in starting the Completion Times for the Required Action. Twenty-four hours is acceptable because it minimizes risk while allowing time for restoration before subjecting the unit to transients associated with shutdown.

The remaining OPERABLE offsite circuit and DGs are adequate to supply electrical power to Train A and Train B of the onsite Class 1E Distribution System. The 24 hour Completion Time takes into account the component OPERABILITY of the redundant counterpart to the inoperable required feature. Additionally, the 24 hour Completion Time takes into account the capacity and capability of the remaining AC sources, a reasonable time for repairs, and the low probability of a DBA occurring during this period.

A.3

According to Regulatory Guide 1.93 (Ref. 6), operation may continue in Condition A for a period that should not exceed 72 hours. With one offsite circuit inoperable, the reliability of the offsite system is degraded, and the potential for a loss of offsite power is increased, with attendant potential for a challenge to the unit safety systems. In this Condition, however, the remaining OPERABLE offsite circuit and DGs are adequate to supply electrical power to the onsite Class 1E Distribution System.

The 72 hour Completion Time takes into account the capacity and capability of the remaining AC sources, a reasonable time for repairs, and the low probability of a DBA occurring during this period.

B.1

To ensure a highly reliable power source remains with an inoperable DG, it is necessary to verify the availability of the offsite circuits on a more frequent basis. Since the Required Action only specifies "perform," a failure of SR 3.8.1.1 acceptance criteria does not result in a Required Action being not met. However, if a circuit fails to pass SR 3.8.1.1, it is inoperable. Upon offsite circuit inoperability, additional Conditions and Required Actions must then be entered.

BASES

ACTIONS (continued)

----------------------------------REVIEWER'S NOTE-----------------------------------
The turbine driven auxiliary feedwater pump is only required to be considered a redundant required feature, and, therefore, required to be determined OPERABLE by this Required Action, if the design is such that the remaining OPERABLE motor or turbine driven auxiliary feedwater pump(s) is not by itself capable (without any reliance on the motor driven auxiliary feedwater pump powered by the emergency bus associated with the inoperable diesel generator) of providing 100% of the auxiliary feedwater flow assumed in the safety analysis.

B.2

Required Action B.2 is intended to provide assurance that a loss of offsite power, during the period that a DG is inoperable, does not result in a complete loss of safety function of critical systems. These features are designed with redundant safety related trains. This includes motor driven auxiliary feedwater pumps. Single train systems, such as turbine driven auxiliary feedwater pumps, are not included. Redundant required feature failures consist of inoperable features with a train, redundant to the train that has an inoperable DG.

The Completion Time for Required Action B.2 is intended to allow the operator time to evaluate and repair any discovered inoperabilities. This Completion Time also allows for an exception to the normal "time zero" for beginning the allowed outage time "clock." In this Required Action, the Completion Time only begins on discovery that both:

a. An inoperable DG exists and

b. A required feature on the other train is inoperable.

If at any time during the existence of this Condition (one DG inoperable) a required feature subsequently becomes inoperable, this Completion Time begins to be tracked.

BASES

ACTIONS (continued)

Discovering one required DG inoperable coincident with one or more inoperable required support or supported features, or both, that are associated with the OPERABLE DG, results in starting the Completion Time for the Required Action. Four hours from the discovery of these events existing concurrently, is acceptable because it minimizes risk while allowing time for restoration before subjecting the unit to transients associated with shutdown.

In this Condition, the remaining OPERABLE DG and offsite circuits are adequate to supply electrical power to the onsite Class 1E Distribution System. Thus, on a component basis, single failure protection for the required feature's function may have been lost; however, function has not been lost. The 4 hour Completion Time takes into account the OPERABILITY of the redundant counterpart to the inoperable required feature. Additionally, the 4 hour Completion Time takes into account the capacity and capability of the remaining AC sources, a reasonable time for repairs, and the low probability of a DBA occurring during this period.

B.3.1 and B.3.2

Required Action B.3.1 provides an allowance to avoid unnecessary testing of OPERABLE DGs. If it can be determined that the cause of the inoperable DG does not exist on the OPERABLE DG, SR 3.8.1.2 does not have to be performed. If the cause of inoperability exists on other DG(s), the other DG(s) would be declared inoperable upon discovery and Condition E of LCO 3.8.1 would be entered. Once the failure is repaired, the common cause failure no longer exists and Required Action B.3.1 is satisfied. If the cause of the initial inoperable DG cannot be confirmed not to exist on the remaining DG(s), performance of SR 3.8.1.2 suffices to provide assurance of continued OPERABILITY of that DG.

In the event the inoperable DG is restored to OPERABLE status prior to completing either B.3.1 or B.3.2, the [plant corrective action program] will continue to evaluate the common cause possibility. This continued evaluation, however, is no longer under the 24 hour constraint imposed while in Condition B.

According to Generic Letter 84-15 (Ref. 7), [24] hours is reasonable to confirm that the OPERABLE DG(s) is not affected by the same problem as the inoperable DG.

BASES

ACTIONS (continued)

B.4

According to Regulatory Guide 1.93 (Ref. 6), operation may continue in Condition B for a period that should not exceed 72 hours.

In Condition B, the remaining OPERABLE DG and offsite circuits are adequate to supply electrical power to the onsite Class 1E Distribution System. The 72 hour Completion Time takes into account the capacity and capability of the remaining AC sources, a reasonable time for repairs, and the low probability of a DBA occurring during this period.

C.1 and C.2

Required Action C.1, which applies when two offsite circuits are inoperable, is intended to provide assurance that an event with a coincident single failure will not result in a complete loss of redundant required safety functions. The Completion Time for this failure of redundant required features is reduced to 12 hours from that allowed for one train without offsite power (Required Action A.2). The rationale for the reduction to 12 hours is that Regulatory Guide 1.93 (Ref. 6) allows a Completion Time of 24 hours for two required offsite circuits inoperable, based upon the assumption that two complete safety trains are OPERABLE. When a concurrent redundant required feature failure exists, this assumption is not the case, and a shorter Completion Time of 12 hours is appropriate. These features are powered from redundant AC safety trains. This includes motor driven auxiliary feedwater pumps. Single train features, such as turbine driven auxiliary pumps, are not included in the list.

The Completion Time for Required Action C.1 is intended to allow the operator time to evaluate and repair any discovered inoperabilities. This Completion Time also allows for an exception to the normal "time zero" for beginning the allowed outage time "clock." In this Required Action, the Completion Time only begins on discovery that both:

a. All required offsite circuits are inoperable and

b. A required feature is inoperable.

BASES

ACTIONS (continued)

If at any time during the existence of Condition C (two offsite circuits inoperable) and a required feature becomes inoperable, this Completion Time begins to be tracked.

According to Regulatory Guide 1.93 (Ref. 6), operation may continue in Condition C for a period that should not exceed 24 hours. This level of degradation means that the offsite electrical power system does not have the capability to effect a safe shutdown and to mitigate the effects of an accident; however, the onsite AC sources have not been degraded. This level of degradation generally corresponds to a total loss of the immediately accessible offsite power sources.

Because of the normally high availability of the offsite sources, this level of degradation may appear to be more severe than other combinations of two AC sources inoperable that involve one or more DGs inoperable. However, two factors tend to decrease the severity of this level of degradation:

a. The configuration of the redundant AC electrical power system that remains available is not susceptible to a single bus or switching failure and

b. The time required to detect and restore an unavailable offsite power source is generally much less than that required to detect and restore an unavailable onsite AC source.

With both of the required offsite circuits inoperable, sufficient onsite AC sources are available to maintain the unit in a safe shutdown condition in the event of a DBA or transient. In fact, a simultaneous loss of offsite AC sources, a LOCA, and a worst case single failure were postulated as a part of the design basis in the safety analysis. Thus, the 24 hour Completion Time provides a period of time to effect restoration of one of the offsite circuits commensurate with the importance of maintaining an AC electrical power system capable of meeting its design criteria.

According to Reference 6, with the available offsite AC sources, two less than required by the LCO, operation may continue for 24 hours. If two offsite sources are restored within 24 hours, unrestricted operation may continue. If only one offsite source is restored within 24 hours, power operation continues in accordance with Condition A.

BASES

ACTIONS (continued)

D.1 and D.2

Pursuant to LCO 3.0.6, the Distribution System ACTIONS would not be entered even if all AC sources to it were inoperable resulting in de-energization. Therefore, the Required Actions of Condition D are modified by a Note to indicate that when Condition D is entered with no AC source to any train, the Conditions and Required Actions for LCO 3.8.9, "Distribution Systems - Operating," must be immediately entered. This allows Condition D to provide requirements for the loss of one offsite circuit and one DG without regard to whether a train is de-energized. LCO 3.8.9 provides the appropriate restrictions for a de-energized train.

According to Regulatory Guide 1.93 (Ref. 6), operation may continue in Condition D for a period that should not exceed 12 hours.

In Condition D, individual redundancy is lost in both the offsite electrical power system and the onsite AC electrical power system. Since power system redundancy is provided by two diverse sources of power, however, the reliability of the power systems in this Condition may appear higher than that in Condition C (loss of both required offsite circuits). This difference in reliability is offset by the susceptibility of this power system configuration to a single bus or switching failure. The 12 hour Completion Time takes into account the capacity and capability of the remaining AC sources, a reasonable time for repairs, and the low probability of a DBA occurring during this period.

E.1

With Train A and Train B DGs inoperable, there are no remaining standby AC sources. Thus, with an assumed loss of offsite electrical power, insufficient standby AC sources are available to power the minimum required ESF functions. Since the offsite electrical power system is the only source of AC power for this level of degradation, the risk associated with continued operation for a short time could be less than that associated with an immediate controlled shutdown (the immediate shutdown could cause grid instability, which could result in a total loss of AC power). Since any inadvertent generator trip could also result in a total loss of offsite AC power, however, the time allowed for continued operation is severely restricted. The intent here is to avoid the risk associated with an immediate controlled shutdown and to minimize the risk associated with this level of degradation.

BASES

ACTIONS (continued)

According to Regulatory Guide 1.93 (Ref. 6), with both DGs inoperable, operation may continue for a period that should not exceed 2 hours.

[F.1

The sequencer(s) is an essential support system to [both the offsite circuit and the DG associated with a given ESF bus]. [Furthermore, the sequencer is on the primary success path for most major AC electrically powered safety systems powered from the associated ESF bus.] Therefore, loss of an [ESF bus sequencer] affects every major ESF system in the [division]. The [12] hour Completion Time provides a period of time to correct the problem commensurate with the importance of maintaining sequencer OPERABILITY. This time period also ensures that the probability of an accident (requiring sequencer OPERABILITY) occurring during periods when the sequencer is inoperable is minimal.

This Condition is preceded by a Note that allows the Condition to be deleted if the unit design is such that any sequencer failure mode will only affect the ability of the associated DG to power its respective safety loads under any conditions. Implicit in this Note is the concept that the Condition must be retained if any sequencer failure mode results in the inability to start all or part of the safety loads when required, regardless of power availability, or results in overloading the offsite power circuit to a safety bus during an event, thereby causing its failure. Also implicit in the Note, is that the Condition is not applicable to any train that does not have a sequencer.]

G.1 and G.2

If the inoperable AC electrical power sources cannot be restored to OPERABLE status within the required Completion Time, the unit must be brought to a MODE in which the LCO does not apply. To achieve this status, the unit must be brought to at least MODE 3 within 6 hours and to MODE 5 within 36 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required unit conditions from full power conditions in an orderly manner and without challenging unit systems.

BASES

ACTIONS (continued)

H.1

Condition H corresponds to a level of degradation in which all redundancy in the AC electrical power supplies has been lost. At this severely degraded level, any further losses in the AC electrical power system will cause a loss of function. Therefore, no additional time is justified for continued operation. The unit is required by LCO 3.0.3 to commence a controlled shutdown.

SURVEILLANCE REQUIREMENTS

The AC sources are designed to permit inspection and testing of all important areas and features, especially those that have a standby function, in accordance with 10 CFR 50, Appendix A, GDC 18 (Ref. 8). Periodic component tests are supplemented by extensive functional tests during refueling outages (under simulated accident conditions). The SRs for demonstrating the OPERABILITY of the DGs are in accordance with the recommendations of Regulatory Guide 1.9 (Ref. 3), Regulatory Guide 1.108 (Ref. 9), and Regulatory Guide 1.137 (Ref. 10), as addressed in the FSAR.

Where the SRs discussed herein specify voltage and frequency tolerances, the following is applicable. The minimum steady state output voltage of [3740] V is 90% of the nominal 4160 V output voltage. This value, which is specified in ANSI C84.1-1982 (Ref. 11), allows for voltage drop to the terminals of 4000 V motors whose minimum operating voltage is specified as 90% or 3600 V. It also allows for voltage drops to motors and other equipment down through the 120 V level where minimum operating voltage is also usually specified as 80% of name plate rating. The specified maximum steady state output voltage of [4756] V is equal to the maximum operating voltage specified for 4000 V motors. It ensures that for a lightly loaded distribution system, the voltage at the terminals of 4000 V motors is no more than the maximum rated operating voltages. The specified minimum and maximum frequencies of the DG are 58.8 Hz and 61.2 Hz, respectively. These values are equal to ± 2% of the 60 Hz nominal frequency and are derived from the recommendations given in Regulatory Guide 1.9 (Ref. 3).

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.8.1.1

This SR assures proper circuit continuity for the offsite AC electrical power supply to the onsite distribution network and availability of offsite AC electrical power. The breaker alignment verifies that each breaker is in its correct position to ensure that distribution buses and loads are connected to their preferred power source, and that appropriate independence of offsite circuits is maintained. The 7 day Frequency is adequate since breaker position is not likely to change without the operator being aware of it and because its status is displayed in the control room.

SR 3.8.1.2 and SR 3.8.1.7

These SRs help to ensure the availability of the standby electrical power supply to mitigate DBAs and transients and to maintain the unit in a safe shutdown condition.

To minimize the wear on moving parts that do not get lubricated when the engine is not running, these SRs are modified by a Note (Note 1 for SR 3.8.1.2 and Note for SR 3.8.1.7) to indicate that all DG starts for these Surveillances may be preceded by an engine prelube period and followed by a warmup period prior to loading by an engine prelube period.

For the purposes of SR 3.8.1.2 and SR 3.8.1.7 testing, the DGs are started from standby conditions. Standby conditions for a DG mean the diesel engine coolant and oil are being continuously circulated and temperature is being maintained consistent with manufacturer recommendations.

[In order to reduce stress and wear on diesel engines, the DG manufacturers recommend a modified start in which the starting speed of DGs is limited, warmup is limited to this lower speed, and the DGs are gradually accelerated to synchronous speed prior to loading. This is the intent of Note 2, which is only applicable when such modified start procedures are recommended by the manufacturer.

SR 3.8.1.7 requires that, at a 184 day Frequency, the DG starts from standby conditions and achieves required voltage and frequency within 10 seconds. The 10 second start requirement supports the assumptions of the design basis LOCA analysis in the FSAR, Chapter [15] (Ref. 5).]

BASES

SURVEILLANCE REQUIREMENTS (continued)

The 10 second start requirement is not applicable to SR 3.8.1.2 (see Note 2) when a modified start procedure as described above is used. If a modified start is not used, 10 second start requirement of SR 3.8.1.7 applies.

Since SR 3.8.1.7 requires a 10 second start, it is more restrictive than SR 3.8.1.2, and it may be performed in lieu of SR 3.8.1.2.

In addition to the SR requirements, the time for the DG to reach steady state operation, unless the modified DG start method is employed, is periodically monitored and the trend evaluated to identify degradation of governor and voltage regulator performance.

The 31 day Frequency for SR 3.8.1.2 is consistent with Regulatory Guide 1.9 (Ref. 3). The 184 day Frequency for SR 3.8.1.7 is a reduction in cold testing consistent with Generic Letter 84-15 (Ref. 7). These Frequencies provide adequate assurance of DG OPERABILITY, while minimizing degradation resulting from testing.

<u>SR 3.8.1.3</u>

This Surveillance verifies that the DGs are capable of synchronizing with the offsite electrical system and accepting loads greater than or equal to the equivalent of the maximum expected accident loads. A minimum run time of 60 minutes is required to stabilize engine temperatures, while minimizing the time that the DG is connected to the offsite source.

Although no power factor requirements are established by this SR, the DG is normally operated at a power factor between [0.8 lagging] and [1.0]. The 0.8 value is the design rating of the machine, while [1.0] is an operational limitation [to ensure circulating currents are minimized]. The 31 day Frequency for this Surveillance is consistent with Regulatory Guide 1.9 (Ref. 3).

This SR is modified by four Notes. Note 1 indicates that diesel engine runs for this Surveillance may include gradual loading, as recommended by the manufacturer, so that mechanical stress and wear on the diesel engine are minimized. Note 2 states that momentary transients because of changing bus loads do not invalidate this test. Similarly, momentary power factor transients above the limit will not invalidate the test. Note 3 indicates that this Surveillance should be conducted on only one DG at a time in order to avoid common cause failures that might result from offsite circuit or grid perturbations. Note 4 stipulates a prerequisite requirement for performance of this SR. A successful DG start must precede this test to credit satisfactory performance.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.8.1.4

This SR provides verification that the level of fuel oil in the day tank [and engine mounted tank] is at or above the level at which fuel oil is automatically added. The level is expressed as an equivalent volume in gallons, and is selected to ensure adequate fuel oil for a minimum of 1 hour of DG operation at full load plus 10%.

The 31 day Frequency is adequate to assure that a sufficient supply of fuel oil is available, since low level alarms are provided and unit operators would be aware of any large uses of fuel oil during this period.

SR 3.8.1.5

Microbiological fouling is a major cause of fuel oil degradation. There are numerous bacteria that can grow in fuel oil and cause fouling, but all must have a water environment in order to survive. Removal of water from the fuel oil day [and engine mounted] tanks once every [31] days eliminates the necessary environment for bacterial survival. This is the most effective means of controlling microbiological fouling. In addition, it eliminates the potential for water entrainment in the fuel oil during DG operation. Water may come from any of several sources, including condensation, ground water, rain water, contaminated fuel oil, and from breakdown of the fuel oil by bacteria. Frequent checking for and removal of accumulated water minimizes fouling and provides data regarding the watertight integrity of the fuel oil system. The Surveillance Frequencies are established by Regulatory Guide 1.137 (Ref. 10). This SR is for preventive maintenance. The presence of water does not necessarily represent failure of this SR provided the accumulated water is removed during the performance of this Surveillance.

SR 3.8.1.6

This Surveillance demonstrates that each required fuel oil transfer pump operates and transfers fuel oil from its associated storage tank to its associated day tank. This is required to support continuous operation of standby power sources. This Surveillance provides assurance that the fuel oil transfer pump is OPERABLE, the fuel oil piping system is intact, the fuel delivery piping is not obstructed, and the controls and control systems for automatic fuel transfer systems are OPERABLE.

SURVEILLANCE REQUIREMENTS (continued)

[The Frequency for this SR is variable, depending on individual system design, with up to a [92] day interval. The [92] day Frequency corresponds to the testing requirements for pumps as contained in the ASME Code (Ref. 12); however, the design of fuel transfer systems is such that pumps will operate automatically or must be started manually in order to maintain an adequate volume of fuel oil in the day [and engine mounted] tanks during or following DG testing. In such a case, a 31 day Frequency is appropriate. Since proper operation of fuel transfer systems is an inherent part of DG OPERABILITY, the Frequency of this SR should be modified to reflect individual designs.]

SR 3.8.1.7

See SR 3.8.1.2.

[SR 3.8.1.8

Transfer of each [4.16 kV ESF bus] power supply from the normal offsite circuit to the alternate offsite circuit demonstrates the OPERABILITY of the alternate circuit distribution network to power the shutdown loads. The [18 month] Frequency of the Surveillance is based on engineering judgment, taking into consideration the unit conditions required to perform the Surveillance, and is intended to be consistent with expected fuel cycle lengths. Operating experience has shown that these components usually pass the SR when performed at the [18 month] Frequency. Therefore, the Frequency was concluded to be acceptable from a reliability standpoint.

This SR is modified by a Note. The reason for the Note is that during operation with the reactor critical, performance of this SR could cause perturbations to the electrical distribution systems that could challenge continued steady state operation and, as a result, unit safety systems. This restriction from normally performing the Surveillance in MODE 1 or 2 is further amplified to allow the Surveillance to be performed for the purpose of reestablishing OPERABILITY (e.g., post work testing following corrective maintenance, corrective modification, deficient or incomplete surveillance testing, and other unanticipated OPERABILITY concerns) provided an assessment determines plant safety is maintained or enhanced. This assessment shall, as a minimum, consider the potential outcomes and transients associated with a failed Surveillance, a successful Surveillance, and a perturbation of the offsite or onsite system

BASES

SURVEILLANCE REQUIREMENTS (continued)

when they are tied together or operated independently for the Surveillance; as well as the operator procedures available to cope with these outcomes. These shall be measured against the avoided risk of a plant shutdown and startup to determine that plant safety is maintained or enhanced when the Surveillance is performed in MODE 1 or 2. Risk insights or deterministic methods may be used for this assessment. Credit may be taken for unplanned events that satisfy this SR .]

SR 3.8.1.9

Each DG is provided with an engine overspeed trip to prevent damage to the engine. Recovery from the transient caused by the loss of a large load could cause diesel engine overspeed, which, if excessive, might result in a trip of the engine. This Surveillance demonstrates the DG load response characteristics and capability to reject the largest single load without exceeding predetermined voltage and frequency and while maintaining a specified margin to the overspeed trip. [For this unit, the single load for each DG and its horsepower rating is as follows:] This Surveillance may be accomplished by:

a. Tripping the DG output breaker with the DG carrying greater than or equal to its associated single largest post-accident load while paralleled to offsite power or while solely supplying the bus, or

b. Tripping its associated single largest post-accident load with the DG solely supplying the bus.

As required by IEEE-308 (Ref. 13), the load rejection test is acceptable if the increase in diesel speed does not exceed 75% of the difference between synchronous speed and the overspeed trip setpoint, or 15% above synchronous speed, whichever is lower.

The time, voltage, and frequency tolerances specified in this SR are derived from Regulatory Guide 1.9 (Ref. 3) recommendations for response during load sequence intervals. The [3] seconds specified is equal to 60% of a typical 5 second load sequence interval associated with sequencing of the largest load. The voltage and frequency specified are consistent with the design range of the equipment powered by the DG. SR 3.8.1.9.a corresponds to the maximum frequency excursion, while SR 3.8.1.9.b and SR 3.8.1.9.c are steady state voltage and frequency values to which the system must recover following load rejection. The [18 month] Frequency is consistent with the recommendation of Regulatory Guide 1.108 (Ref. 9).

BASES

SURVEILLANCE REQUIREMENTS (continued)

This SR is modified by two Notes. The reason for Note 1 is that during operation with the reactor critical, performance of this SR could cause perturbations to the electrical distribution systems that could challenge continued steady state operation and, as a result, unit safety systems. This restriction from normally performing the Surveillance in MODE 1 or 2 is further amplified to allow the Surveillance to be performed for the purpose of reestablishing OPERABILITY (e.g., post work testing following corrective maintenance, corrective modification, deficient or incomplete surveillance testing, and other unanticipated OPERABILITY concerns) provided an assessment determines plant safety is maintained or enhanced. This assessment shall, as a minimum, consider the potential outcomes and transients associated with a failed Surveillance, a successful Surveillance, and a perturbation of the offsite or onsite system when they are tied together or operated independently for the Surveillance; as well as the operator procedures available to cope with these outcomes. These shall be measured against the avoided risk of a plant shutdown and startup to determine that plant safety is maintained or enhanced when the Surveillance is performed in MODE 1 or 2. Risk insights or deterministic methods may be used for this assessment. Credit may be taken for unplanned events that satisfy this SR. Note 2 ensures that the DG is tested under load conditions that are as close to design basis conditions as possible. When synchronized with offsite power, testing should be performed at a power factor of ≤ [0.9]. This power factor is representative of the actual inductive loading a DG would see under design basis accident conditions. Under certain conditions, however, Note 2 allows the Surveillance to be conducted at a power factor other than ≤ [0.9]. These conditions occur when grid voltage is high, and the additional field excitation needed to get the power factor to ≤ [0.9] results in voltages on the emergency busses that are too high. Under these conditions, the power factor should be maintained as close as practicable to [0.9] while still maintaining acceptable voltage limits on the emergency busses. In other circumstances, the grid voltage may be such that the DG excitation levels needed to obtain a power factor of [0.9] may not cause unacceptable voltages on the emergency busses, but the excitation levels are in excess of those recommended for the DG. In such cases, the power factor shall be maintained as close as practicable to [0.9] without exceeding the DG excitation limits.

-----------------------------------REVIEWER'S NOTE-----------------------------------
The above MODE restrictions may be deleted if it can be demonstrated to the staff, on a plant specific basis, that performing the SR with the reactor in any of the restricted MODES can satisfy the following criteria, as applicable:

a. Performance of the SR will not render any safety system or component inoperable, SURVEILLANCE REQUIREMENTS (continued)

b. Performance of the SR will not cause perturbations to any of the electrical distribution systems that could result in a challenge to steady state operation or to plant safety systems, and

c. Performance of the SR or failure of the SR will not cause or result in an AOO with attendant challenge to plant safety systems.

SR 3.8.1.10

This Surveillance demonstrates the DG capability to reject a full load without overspeed tripping or exceeding the predetermined voltage limits. The DG full load rejection may occur because of a system fault or inadvertent breaker tripping. This Surveillance ensures proper engine generator load response under the simulated test conditions. This test simulates the loss of the total connected load that the DG experiences following a full load rejection and verifies that the DG will not trip upon loss of the load. These acceptance criteria provide DG damage protection. While the DG is not expected to experience this transient during an event and continues to be available, this response ensures that the DG is not degraded for future application, including reconnection to the bus if the trip initiator can be corrected or isolated.

The [18 month] Frequency is consistent with the recommendation of Regulatory Guide 1.108 (Ref. 9) and is intended to be consistent with expected fuel cycle lengths.

This SR is modified by two Notes. The reason for Note 1 is that during operation with the reactor critical, performance of this SR could cause perturbation to the electrical distribution systems that could challenge continued steady state operation and, as a result, unit safety systems. This restriction from normally performing the Surveillance in MODE 1 or 2 is further amplified to allow the Surveillance to be performed for the purpose of reestablishing OPERABILITY (e.g., post work testing following corrective maintenance, corrective modification, deficient or incomplete surveillance testing, and other unanticipated OPERABILITY concerns) provided an assessment determines plant safety is maintained or enhanced. This assessment shall, as a minimum, consider the potential outcomes and transients associated with a failed Surveillance, a successful Surveillance, and a perturbation of the offsite or onsite system when they are tied together or operated independently for the

BASES

SURVEILLANCE REQUIREMENTS (continued)

Surveillance; as well as the operator procedures available to cope with these outcomes. These shall be measured against the avoided risk of a plant shutdown and startup to determine that plant safety is maintained or enhanced when the Surveillance is performed in MODE 1 or 2. Risk insights or deterministic methods may be used for this assessment. Credit may be taken for unplanned events that satisfy this SR. Note 2 ensures that the DG is tested under load conditions that are as close to design basis conditions as possible. When synchronized with offsite power, testing should be performed at a power factor of ≤ [0.9]. This power factor is representative of the actual inductive loading a DG would see under design basis accident conditions. Under certain conditions, however, Note 2 allows the Surveillance to be conducted at a power factor other than ≤ [0.9]. These conditions occur when grid voltage is high, and the additional field excitation needed to get the power factor to ≤ [0.9] results in voltages on the emergency busses that are too high. Under these conditions, the power factor should be maintained as close as practicable to [0.9] while still maintaining acceptable voltage limits on the emergency busses. In other circumstances, the grid voltage may be such that the DG excitation levels needed to obtain a power factor of [0.9] may not cause unacceptable voltages on the emergency busses, but the excitation levels are in excess of those recommended for the DG. In such cases, the power factor shall be maintained as close as practicable to [0.9] without exceeding the DG excitation limits.

----------------------------------REVIEWER'S NOTE----------------------------------
The above MODE restrictions may be deleted if it can be demonstrated to the staff, on a plant specific basis, that performing the SR with the reactor in any of the restricted MODES can satisfy the following criteria, as applicable:

a. Performance of the SR will not render any safety system or component inoperable,

b. Performance of the SR will not cause perturbations to any of the electrical distribution systems that could result in a challenge to steady state operation or to plant safety systems, and

c. Performance of the SR or failure of the SR will not cause or result in an AOO with attendant challenge to plant safety systems.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.8.1.11

As required by Regulatory Guide 1.108 (Ref. 9), paragraph 2.a.(1), this Surveillance demonstrates the as designed operation of the standby power sources during loss of the offsite source. This test verifies all actions encountered from the loss of offsite power, including shedding of the nonessential loads and energization of the emergency buses and respective loads from the DG. It further demonstrates the capability of the DG to automatically achieve the required voltage and frequency within the specified time.

The DG auto-start time of [10] seconds is derived from requirements of the accident analysis to respond to a design basis large break LOCA. The Surveillance should be continued for a minimum of 5 minutes in order to demonstrate that all starting transients have decayed and stability has been achieved.

The requirement to verify the connection and power supply of permanent and auto-connected loads is intended to satisfactorily show the relationship of these loads to the DG loading logic. In certain circumstances, many of these loads cannot actually be connected or loaded without undue hardship or potential for undesired operation. For instance, Emergency Core Cooling Systems (ECCS) injection valves are not desired to be stroked open, high pressure injection systems are not capable of being operated at full flow, or shutdown cooling (SDC) systems performing a decay heat removal function are not desired to be realigned to the ECCS mode of operation. In lieu of actual demonstration of connection and loading of loads, testing that adequately shows the capability of the DG system to perform these functions is acceptable. This testing may include any series of sequential, overlapping, or total steps so that the entire connection and loading sequence is verified.

The Frequency of [18 months] is consistent with the recommendations of Regulatory Guide 1.108 (Ref. 9), paragraph 2.a.(1), takes into consideration unit conditions required to perform the Surveillance, and is intended to be consistent with expected fuel cycle lengths.

This SR is modified by two Notes. The reason for Note 1 is to minimize wear and tear on the DGs during testing. For the purpose of this testing, the DGs must be started from standby conditions, that is, with the engine coolant and oil continuously circulated and temperature maintained

BASES

SURVEILLANCE REQUIREMENTS (continued)

consistent with manufacturer recommendations. The reason for Note 2 is that performing the Surveillance would remove a required offsite circuit from service, perturb the electrical distribution system, and challenge safety systems. This restriction from normally performing the Surveillance in MODE 1 or 2 is further amplified to allow portions of the Surveillance to be performed for the purpose of reestablishing OPERABILITY (e.g., post work testing following corrective maintenance, corrective modification, deficient or incomplete surveillance testing, and other unanticipated OPERABILITY concerns) provided an assessment determines plant safety is maintained or enhanced. This assessment shall, as a minimum, consider the potential outcomes and transients associated with a failed partial Surveillance, a successful partial Surveillance, and a perturbation of the offsite or onsite system when they are tied together or operated independently for the partial Surveillance; as well as the operator procedures available to cope with these outcomes. These shall be measured against the avoided risk of a plant shutdown and startup to determine that plant safety is maintained or enhanced when portions of the Surveillance are performed in MODE 1 or 2. Risk insights or deterministic methods may be used for the assessment. Credit may be taken for unplanned events that satisfy this SR.

[SR 3.8.1.12

This Surveillance demonstrates that the DG automatically starts and achieves the required voltage and frequency within the specified time ([10] seconds) from the design basis actuation signal (LOCA signal) and operates for ≥ 5 minutes. The 5 minute period provides sufficient time to demonstrate stability. SR 3.8.1.12.d and SR 3.8.1.12.e ensure that permanently connected loads and emergency loads are energized from the offsite electrical power system on an ESF signal without loss of offsite power.

The requirement to verify the connection of permanent and autoconnected loads is intended to satisfactorily show the relationship of these loads to the DG loading logic. In certain circumstances, many of these loads cannot actually be connected or loaded without undue hardship or potential for undesired operation. For instance, ECCS injection valves are not desired to be stroked open, high pressure injection systems are not capable of being operated at full flow, or SDC systems performing a decay heat removal function are not desired to be realigned to the ECCS mode of operation. In lieu of actual demonstration

BASES

SURVEILLANCE REQUIREMENTS (continued)

of connection and loading of loads, testing that adequately shows the capability of the DG system to perform these functions is acceptable. This testing may include any series of sequential, overlapping, or total steps so that the entire connection and loading sequence is verified.

The Frequency of [18 months] takes into consideration unit conditions required to perform the Surveillance and is intended to be consistent with the expected fuel cycle lengths. Operating experience has shown that these components usually pass the SR when performed at the [18 month] Frequency. Therefore, the Frequency was concluded to be acceptable from a reliability standpoint.

This SR is modified by two Notes. The reason for Note 1 is to minimize wear and tear on the DGs during testing. For the purpose of this testing, the DGs must be started from standby conditions, that is, with the engine coolant and oil continuously circulated and temperature maintained consistent with manufacturer recommendations. The reason for Note 2 is that during operation with the reactor critical, performance of this Surveillance could cause perturbations to the electrical distribution systems that could challenge continued steady state operation and, as a result, unit safety systems. This restriction from normally performing the Surveillance in MODE 1 or 2 is further amplified to allow portions of the Surveillance to be performed for the purpose of reestablishing OPERABILITY (e.g., post work testing following corrective maintenance, corrective modification, deficient or incomplete surveillance testing, and other unanticipated OPERABILITY concerns) provided an assessment determines plant safety is maintained or enhanced. This assessment shall, as a minimum, consider the potential outcomes and transients associated with a failed partial Surveillance, a successful partial Surveillance, and a perturbation of the offsite or onsite system when they are tied together or operated independently for the partial Surveillance; as well as the operator procedures available to cope with these outcomes. These shall be measured against the avoided risk of a plant shutdown and startup to determine that plant safety is maintained or enhanced when portions of the Surveillance are performed in MODE 1 or . Risk insights or deterministic methods may be used for the assessment. Credit may be taken for unplanned events that satisfy this SR.]

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.8.1.13

This Surveillance demonstrates that DG noncritical protective functions (e.g., high jacket water temperature) are bypassed on a loss of voltage signal concurrent with an ESF actuation test signal. Noncritical automatic trips are all automatic trips except:

a. Engine overspeed;

b. Generator differential current;

[c. Low lube oil pressure;

d. High crankcase pressure; and

e. Start failure relay.]

The noncritical trips are bypassed during DBAs and provide an alarm on an abnormal engine condition. This alarm provides the operator with sufficient time to react appropriately. The DG availability to mitigate the DBA is more critical than protecting the engine against minor problems that are not immediately detrimental to emergency operation of the DG.

The [18 month] Frequency is based on engineering judgment, taking into consideration unit conditions required to perform the Surveillance, and is intended to be consistent with expected fuel cycle lengths. Operating experience has shown that these components usually pass the SR when performed at the [18 month] Frequency. Therefore, the Frequency was concluded to be acceptable from a reliability standpoint.

The SR is modified by a Note. The reason for the Note is that performing the Surveillance would remove a required DG from service. This restriction from normally performing the Surveillance in MODE or is further amplified to allow the Surveillance to be performed for the purpose of reestablishing OPERABILITY (e.g., post work testing following corrective maintenance, corrective modification, deficient or incomplete surveillance testing, and other unanticipated OPERABILITY concerns) provided an assessment determines plant safety is maintained or enhanced. This assessment shall, as a minimum, consider the potential outcomes and transients associated with a failed Surveillance, a successful Surveillance, and a perturbation of the offsite or onsite system when they are tied together or operated independently for the Surveillance; as well as the operator procedures available to cope with these outcomes. These shall be measured against the avoided risk of a plant shutdown and startup to determine that plant safety is maintained or

BASES

SURVEILLANCE REQUIREMENTS (continued)

enhanced when the Surveillance is performed in MODE 1 or 2. Risk insights or deterministic methods may be used for this assessment. Credit may be taken for unplanned events that satisfy this SR.

----------------------------------REVIEWER'S NOTE----------------------------------
The above MODE restrictions may be deleted if it can be demonstrated to the staff, on a plant specific basis, that performing the SR with the reactor in any of the restricted MODES can satisfy the following criteria, as applicable:

a. Performance of the SR will not render any safety system or component inoperable,

b. Performance of the SR will not cause perturbations to any of the electrical distribution systems that could result in a challenge to steady state operation or to plant safety systems, and

c. Performance of the SR or failure of the SR will not cause or result in an AOO with attendant challenge to plant safety systems.

SR 3.8.1.14

Regulatory Guide 1.108 (Ref. 9), paragraph 2.a.(3), requires demonstration once per 18 months that the DGs can start and run continuously at full load capability for an interval of not less than 24 hours, ≥ [2] hours of which is at a load equivalent to 110% of the continuous duty rating and the remainder of the time at a load equivalent to the continuous duty rating of the DG. The DG starts for this Surveillance can be performed either from standby or hot conditions. The provisions for prelubricating and warmup, discussed in SR 3.8.1.2, and for gradual loading, discussed in SR 3.8.1.3, are applicable to this SR.

The load band is provided to avoid routine overloading of the DG. Routine overloading may result in more frequent teardown inspections in accordance with vendor recommendations in order to maintain DG OPERABILITY.

The [18 month] Frequency is consistent with the recommendations of Regulatory Guide 1.108 (Ref. 7), paragraph 2.a.(3), takes into consideration unit conditions required to perform the Surveillance, and is intended to be consistent with expected fuel cycle lengths.

BASES

SURVEILLANCE REQUIREMENTS (continued)

This Surveillance is modified by three Notes. Note 1 states that momentary transients due to changing bus loads do not invalidate this test. Similarly, momentary power factor transients above the power factor limit will not invalidate the test. The reason for Note 2 is that during operation with the reactor critical, performance of this Surveillance could cause perturbations to the electrical distribution systems that could challenge continued steady state operation and, as a result, unit safety systems. This restriction from normally performing the Surveillance in MODE or is further amplified to allow the Surveillance to be performed for the purpose of reestablishing OPERABILITY (e.g., post work testing following corrective maintenance, corrective modification, deficient or incomplete surveillance testing, and other unanticipated OPERABILITY concerns) provided an assessment determines plant safety is maintained or enhanced. This assessment shall, as a minimum, consider the potential outcomes and transients associated with a failed Surveillance, a successful Surveillance, and a perturbation of the offsite or onsite system when they are tied together or operated independently for the Surveillance; as well as the operator procedures available to cope with these outcomes. These shall be measured against the avoided risk of a plant shutdown and startup to determine that plant safety is maintained or enhanced when the Surveillance is performed in MODE or . Risk insights or deterministic methods may be used for this assessment. Credit may be taken for unplanned events that satisfy this SR. Note 3 ensures that the DG is tested under load conditions that are as close to design basis conditions as possible. When synchronized with offsite power, testing should be performed at a power factor of ≤ [0.9]. This power factor is representative of the actual inductive loading a DG would see under design basis accident conditions. Under certain conditions, however, Note 3 allows the Surveillance to be conducted at a power factor other than ≤ [0.9]. These conditions occur when grid voltage is high, and the additional field excitation needed to get the power factor to ≤ [0.9] results in voltages on the emergency busses that are too high. Under these conditions, the power factor should be maintained as close as practicable to [0.9] while still maintaining acceptable voltage limits on the emergency busses. In other circumstances, the grid voltage may be such that the DG excitation levels needed to obtain a power factor of [0.9] may not cause unacceptable voltages on the emergency busses, but the excitation levels are in excess of those recommended for the DG. In such cases, the power factor shall be maintained as close practicable to [0.9] without exceeding the DG excitation limits.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.8.1.15

This Surveillance demonstrates that the diesel engine can restart from a hot condition, such as subsequent to shutdown from normal Surveillances, and achieve the required voltage and frequency within [10] seconds. The [10] second time is derived from the requirements of the accident analysis to respond to a design basis large break LOCA. The [18 month] Frequency is consistent with the recommendations of Regulatory Guide 1.108 (Ref. 9), paragraph 2.a.(5).

This SR is modified by two Notes. Note 1 ensures that the test is performed with the diesel sufficiently hot. The load band is provided to avoid routine overloading of the DG. Routine overloads may result in more frequent teardown inspections in accordance with vendor recommendations in order to maintain DG OPERABILITY. The requirement that the diesel has operated for at least [2] hours at full load conditions prior to performance of this Surveillance is based on manufacturer recommendations for achieving hot conditions. Momentary transients due to changing bus loads do not invalidate this test. Note 2 allows all DG starts to be preceded by an engine prelube period to minimize wear and tear on the diesel during testing.

SR 3.8.1.16

As required by Regulatory Guide 1.108 (Ref. 9), paragraph 2.a.(6), this Surveillance ensures that the manual synchronization and automatic load transfer from the DG to the offsite source can be made and that the DG can be returned to ready to load status when offsite power is restored. It also ensures that the auto-start logic is reset to allow the DG to reload if a subsequent loss of offsite power occurs. The DG is considered to be in ready to load status when the DG is at rated speed and voltage, the output breaker is open and can receive and autoclose signal on bus undervoltage, and the load sequence timers are reset.

The Frequency of [18 months] is consistent with the recommendations of Regulatory Guide 1.108 (Ref. 9), paragraph 2.a.(6), and takes into consideration unit conditions required to perform the Surveillance.

BASES

SURVEILLANCE REQUIREMENTS (continued)

This SR is modified by a Note. The reason for the Note is that performing the Surveillance would remove a required offsite circuit from service, perturb the electrical distribution system, and challenge safety systems. This restriction from normally performing the Surveillance in MODE 1 or 2 is further amplified to allow the Surveillance to be performed for the purpose of reestablishing OPERABILITY (e.g., post work testing following corrective maintenance, corrective modification, deficient or incomplete surveillance testing, and other unanticipated OPERABILITY concerns) provided an assessment determines plant safety is maintained or enhanced. This assessment shall, as a minimum, consider the potential outcomes and transients associated with a failed Surveillance, a successful Surveillance, and a perturbation of the offsite or onsite system when they are tied together or operated independently for the Surveillance; as well as the operator procedures available to cope with these outcomes. These shall be measured against the avoided risk of a plant shutdown and startup to determine that plant safety is maintained or enhanced when the Surveillance is performed in MODE 1 or 2. Risk insights or deterministic methods may be used for this assessment. Credit may be taken for unplanned events that satisfy this SR.

[SR 3.8.1.17

Demonstration of the test mode override ensures that the DG availability under accident conditions will not be compromised as the result of testing and the DG will automatically reset to ready to load operation if a LOCA actuation signal is received during operation in the test mode. Ready to load operation is defined as the DG running at rated speed and voltage with the DG output breaker open. These provisions for automatic switchover are required by IEEE-308 (Ref. 13), paragraph 6.2.6(2).

The requirement to automatically energize the emergency loads with offsite power is essentially identical to that of SR 3.8.1.12. The intent in the requirement associated with SR 3.8.1.17.b is to show that the emergency loading was not affected by the DG operation in test mode. In lieu of actual demonstration of connection and loading of loads, testing that adequately shows the capability of the emergency loads to perform these functions is acceptable. This testing may include any series of sequential, overlapping, or total steps so that the entire connection and loading sequence is verified.

The [18 month] Frequency is consistent with the recommendations of Regulatory Guide 1.108 (Ref. 9), paragraph 2.a.(8); takes into consideration unit conditions required to perform the Surveillance; and is intended to be consistent with expected fuel cycle lengths.

BASES

SURVEILLANCE REQUIREMENTS (continued)

This SR is modified by a Note. The reason for the Note is that performing the Surveillance would remove a required offsite circuit from service, perturb the electrical distribution system, and challenge safety systems. This restriction from normally performing the Surveillance in MODE 1 or 2 is further amplified to allow portions of the Surveillance to be performed for the purpose of reestablishing OPERABILITY (e.g., post work testing following corrective maintenance, corrective modification, deficient or incomplete surveillance testing, and other unanticipated OPERABILITY concerns) provided an assessment determines plant safety is maintained or enhanced. This assessment shall, as a minimum, consider the potential outcomes and transients associated with a failed partial Surveillance, a successful partial Surveillance, and a perturbation of the offsite or onsite system when they are tied together or operated independently for the partial Surveillance; as well as the operator procedures available to cope with these outcomes. These shall be measured against the avoided risk of a plant shutdown and startup to determine that plant safety is maintained or enhanced when portions of the Surveillance are performed in MODE 1 or 2. Risk insights or deterministic methods may be used for the assessment. Credit may be taken for unplanned events that satisfy this SR.]

SR 3.8.1.18

Under accident [and loss of offsite power] conditions loads are sequentially connected to the bus by the [automatic load sequencer]. The sequencing logic controls the permissive and starting signals to motor breakers to prevent overloading of the DGs due to high motor starting currents. The [10]% load sequence time interval tolerance ensures that sufficient time exists for the DG to restore frequency and voltage prior to applying the next load and that safety analysis assumptions regarding ESF equipment time delays are not violated. Reference 1 provides a summary of the automatic loading of ESF buses.

The Frequency of [18 months] is consistent with the recommendations of Regulatory Guide 1.108 (Ref. 9), paragraph 2.a.(2); takes into consideration unit conditions required to perform the Surveillance; and is intended to be consistent with expected fuel cycle lengths.

BASES

SURVEILLANCE REQUIREMENTS (continued)

This SR is modified by a Note. The reason for the Note is that performing the Surveillance would remove a required offsite circuit from service, perturb the electrical distribution system, and challenge safety systems. This restriction from normally performing the Surveillance in MODE 1 or 2 is further amplified to allow the Surveillance to be performed for the purpose of reestablishing OPERABILITY (e.g., post work testing following corrective maintenance, corrective modification, deficient or incomplete surveillance testing, and other unanticipated OPERABILITY concerns) provided an assessment determines plant safety is maintained or enhanced. This assessment shall, as a minimum, consider the potential outcomes and transients associated with a failed Surveillance, a successful Surveillance, and a perturbation of the offsite or onsite system when they are tied together or operated independently for the Surveillance; as well as the operator procedures available to cope with these outcomes. These shall be measured against the avoided risk of a plant shutdown and startup to determine that plant safety is maintained or enhanced when the Surveillance is performed in MODE 1 or 2. Risk insights or deterministic methods may be used for this assessment. Credit may be taken for unplanned events that satisfy this SR.

----------------------------------REVIEWER'S NOTE----------------------------------
The above MODE restrictions may be deleted if it can be demonstrated to the staff, on a plant specific basis, that performing the SR with the reactor in any of the restricted MODES can satisfy the following criteria, as applicable:

a. Performance of the SR will not render any safety system or component inoperable,

b. Performance of the SR will not cause perturbations to any of the electrical distribution systems that could result in a challenge to steady state operation or to plant safety systems, and

c. Performance of the SR or failure of the SR will not cause or result in an AOO with attendant challenge to plant safety systems.

<u>SR 3.8.1.19</u>

In the event of a DBA coincident with a loss of offsite power, the DGs are required to supply the necessary power to ESF systems so that the fuel, RCS, and containment design limits are not exceeded.

BASES

SURVEILLANCE REQUIREMENTS (continued)

This Surveillance demonstrates the DG operation, as discussed in the Bases for SR 3.8.1.11, during a loss of offsite power actuation test signal in conjunction with an ESF actuation signal. In lieu of actual demonstration of connection and loading of loads, testing that adequately shows the capability of the DG system to perform these functions is acceptable. This testing may include any series of sequential, overlapping, or total steps so that the entire connection and loading sequence is verified.

The Frequency of [18 months] takes into consideration unit conditions required to perform the Surveillance and is intended to be consistent with an expected fuel cycle length of [18 months].

This SR is modified by two Notes. The reason for Note 1 is to minimize wear and tear on the DGs during testing. For the purpose of this testing, the DGs must be started from standby conditions, that is, with the engine coolant and oil continuously circulated and temperature maintained consistent with manufacturer recommendations for DGs. The reason for Note 2 is that performing the Surveillance would remove a required offsite circuit from service, perturb the electrical distribution system, and challenge safety systems. This restriction from normally performing the Surveillance in MODE 1 or 2 is further amplified to allow portions of the Surveillance to be performed for the purpose of reestablishing OPERABILITY (e.g., post work testing following corrective maintenance, corrective modification, deficient or incomplete surveillance testing, and other unanticipated OPERABILITY concerns) provided an assessment determines plant safety is maintained or enhanced. This assessment shall, as a minimum, consider the potential outcomes and transients associated with a failed partial Surveillance, a successful partial Surveillance, and a perturbation of the offsite or onsite system when they are tied together or operated independently for the partial Surveillance; as well as the operator procedures available to cope with these outcomes. These shall be measured against the avoided risk of a plant shutdown and startup to determine that plant safety is maintained or enhanced when portions of the Surveillance are performed in MODE 1 or 2. Risk insights or deterministic methods may be used for the assessment. Credit may be taken for unplanned events that satisfy this SR.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.8.1.20

This Surveillance demonstrates that the DG starting independence has not been compromised. Also, this Surveillance demonstrates that each engine can achieve proper speed within the specified time when the DGs are started simultaneously.

The 10 year Frequency is consistent with the recommendations of Regulatory Guide 1.108 (Ref. 9).

This SR is modified by a Note. The reason for the Note is to minimize wear on the DG during testing. For the purpose of this testing, the DGs must be started from standby conditions, that is, with the engine coolant and oil continuously circulated, and temperature maintained consistent with manufacturer recommendations.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 17.
2. FSAR, Chapter [8].
3. Regulatory Guide 1.9, Rev. [3].
4. FSAR, Chapter [6].
5. FSAR, Chapter [15].
6. Regulatory Guide 1.93, Rev. [ ], [date].
7. Generic Letter 84-15.
8. 10 CFR 50, Appendix A, GDC 18.
9. Regulatory Guide 1.108, Rev. [1], [August 1977].
10. Regulatory Guide 1.137, Rev. [ ], [date].
11. ANSI C84.1-1982.
12. ASME Code for Operation and Maintenance of Nuclear Power Plants.
13. IEEE Standard 308-[1978].

B 3.8 ELECTRICAL POWER SYSTEMS

B 3.8.2 AC Sources - Shutdown

BASES

BACKGROUND

A description of the AC sources is provided in the Bases for LCO 3.8.1, "AC Sources - Operating."

APPLICABLE SAFETY ANALYSES

The OPERABILITY of the minimum AC sources during MODES 5 and 6 and during movement of [recently] irradiated fuel assemblies ensures that:

a. The unit can be maintained in the shutdown or refueling condition for extended periods,

b. Sufficient instrumentation and control capability is available for monitoring and maintaining the unit status, and

c. Adequate AC electrical power is provided to mitigate events postulated during shutdown, such as a fuel handling accident [involving handling recently irradiated fuel. Due to radioactive decay, AC electrical power is only required to mitigate fuel handling accidents involving handling recently irradiated fuel (i.e., fuel that has occupied part of a critical reactor core within the previous [X] days)].

In general, when the unit is shut down, the Technical Specifications requirements ensure that the unit has the capability to mitigate the consequences of postulated accidents. However, assuming a single failure and concurrent loss of all offsite or all onsite power is not required. The rationale for this is based on the fact that many Design Basis Accidents (DBAs) that are analyzed in MODES 1, 2, 3, and 4 have no specific analyses in MODES 5 and 6. Worst case bounding events are deemed not credible in MODES 5 and 6 because the energy contained within the reactor pressure boundary, reactor coolant temperature and pressure, and the corresponding stresses result in the probabilities of occurrence being significantly reduced or eliminated, and in minimal consequences. These deviations from DBA analysis assumptions and design requirements during shutdown conditions are allowed by the LCO for required systems.

BASES

APPLICABLE SAFETY ANALYSES (continued)

During MODES 1, 2, 3, and 4, various deviations from the analysis assumptions and design requirements are allowed within the Required Actions. This allowance is in recognition that certain testing and maintenance activities must be conducted provided an acceptable level of risk is not exceeded. During MODES 5 and 6, performance of a significant number of required testing and maintenance activities is also required. In MODES 5 and 6, the activities are generally planned and administratively controlled. Relaxations from MODE 1, 2, 3, and 4 LCO requirements are acceptable during shutdown modes based on:

a. The fact that time in an outage is limited. This is a risk prudent goal as well as a utility economic consideration.

b. Requiring appropriate compensatory measures for certain conditions. These may include administrative controls, reliance on systems that do not necessarily meet typical design requirements applied to systems credited in operating MODE analyses, or both.

c. Prudent utility consideration of the risk associated with multiple activities that could affect multiple systems.

d. Maintaining, to the extent practical, the ability to perform required functions (even if not meeting MODE 1, 2, 3, and 4 OPERABILITY requirements) with systems assumed to function during an event.

In the event of an accident during shutdown, this LCO ensures the capability to support systems necessary to avoid immediate difficulty, assuming either a loss of all offsite power or a loss of all onsite diesel generator (DG) power.

The AC sources satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

One offsite circuit capable of supplying the onsite Class 1E power distribution subsystem(s) of LCO 3.8.10, "Distribution Systems - Shutdown," ensures that all required loads are powered from offsite power. An OPERABLE DG, associated with a distribution system train required to be OPERABLE by LCO 3.8.10, ensures a diverse power source is available to provide electrical power support, assuming a loss of the offsite circuit. Together, OPERABILITY of the required offsite circuit and DG ensures the availability of sufficient AC sources to operate the unit in a safe manner and to mitigate the consequences of postulated events during shutdown (e.g., fuel handling accidents [involving handling recently irradiated fuel]).

BASES

LCO (continued)

The qualified offsite circuit must be capable of maintaining rated frequency and voltage, and accepting required loads during an accident, while connected to the Engineered Safety Feature (ESF) bus(es). Qualified offsite circuits are those that are described in the FSAR and are part of the licensing basis for the unit.

[Offsite circuit #1 consists of Safeguards Transformer B, which is supplied from Switchyard Bus B, and is fed through breaker 52-3 powering the ESF transformer XNBO1, which, in turn, powers the #1 ESF bus through its normal feeder breaker. The second offsite circuit consists of the Startup Transformer, which is normally fed from the Switchyard Bus A, and is fed through breaker PA 0201 powering the ESF transformer, which, in turn, powers the #2 ESF bus through its normal feeder breaker.]

The DG must be capable of starting, accelerating to rated speed and voltage, connecting to its respective ESF bus on detection of bus undervoltage, and accepting required loads. This sequence must be accomplished within [10] seconds. The DG must be capable of accepting required loads within the assumed loading sequence intervals, and must continue to operate until offsite power can be restored to the ESF buses. These capabilities are required to be met from a variety of initial conditions such as DG in standby with the engine hot and DG in standby at ambient conditions.

Proper sequencing of loads, including tripping of nonessential loads, is a required function for DG OPERABILITY.

[In addition, proper sequencer operation is an integral part of offsite circuit OPERABILITY since its inoperability impacts on the ability to start and maintain energized loads required OPERABLE by LCO 3.8.10.]

It is acceptable for trains to be cross tied during shutdown conditions, allowing a single offsite power circuit to supply all required trains.

APPLICABILITY

The AC sources required to be OPERABLE in MODES 5 and 6 and during movement of [recently] irradiated fuel assemblies provide assurance that:

a. Systems to provide adequate coolant inventory makeup are available for the irradiated fuel assemblies,

BASES

APPLICABILITY (continued)

b. Systems needed to mitigate a fuel handling accident [involving handling [recently] irradiated fuel (i.e., fuel that has occupied part of a critical reactor core within the previous [X] days)] are available,

c. Systems necessary to mitigate the effects of events that can lead to core damage during shutdown are available, and

d. Instrumentation and control capability is available for monitoring and maintaining the unit in a cold shutdown condition or refueling condition.

The AC power requirements for MODES 1, 2, 3, and 4 are covered in LCO 3.8.1.

ACTIONS

LCO 3.0.3 is not applicable while in MODE 5 or 6. However, since irradiated fuel assembly movement can occur in MODE 1, 2, 3, or 4, the ACTIONS have been modified by a Note stating that LCO 3.0.3 is not applicable. If moving irradiated fuel assemblies while in MODE 5 or 6, LCO 3.0.3 would not specify any action. If moving irradiated fuel assemblies while in MODE 1, 2, 3, or 4, the fuel movement is independent of reactor operations. Entering LCO 3.0.3, while in MODE 1, 2, 3, or 4 would require the unit to be shutdown unnecessarily.

A.1

An offsite circuit would be considered inoperable if it were not available to one required ESF train. Although two trains may be required by LCO 3.8.10, the remaining train with offsite power available may be capable of supporting sufficient required features to allow continuation of CORE ALTERATIONS and [recently] irradiated fuel movement. By the allowance of the option to declare required features inoperable, with no offsite power available, appropriate restrictions will be implemented in accordance with the affected required features LCO's ACTIONS.

A.2.1, A.2.2, A.2.3, A.2.4, B.1, B.2, B.3, and B.4

With the offsite circuit not available to all required trains, the option would still exist to declare all required features inoperable. Since this option may involve undesired administrative efforts, the allowance for sufficiently conservative actions is made. With the required DG inoperable, the

BASES

ACTIONS (continued)

minimum required diversity of AC power sources is not available. It is, therefore, required to suspend CORE ALTERATIONS, movement of [recently] irradiated fuel assemblies, and operations involving positive reactivity additions that could result in loss of required SDM (MODE 5) or boron concentration (MODE 6). Suspending positive reactivity additions that could result in failure to meet the minimum SDM or boron concentration limit is required to assure continued safe operation. Introduction of coolant inventory must be from sources that have a boron concentration greater than that what would be required in the RCS for minimum SDM or refueling boron concentration. This may result in an overall reduction in RCS boron concentration, but provides acceptable margin to maintaining subcritical operation. Introduction of temperature changes including temperature increases when operating with a positive MTC must also be evaluated to ensure they do not result in a loss of required SDM.

Suspension of these activities does not preclude completion of actions to establish a safe conservative condition. These actions minimize the probability or the occurrence of postulated events. It is further required to immediately initiate action to restore the required AC sources and to continue this action until restoration is accomplished in order to provide the necessary AC power to the unit safety systems.

The Completion Time of immediately is consistent with the required times for actions requiring prompt attention. The restoration of the required AC electrical power sources should be completed as quickly as possible in order to minimize the time during which the unit safety systems may be without sufficient power.

Pursuant to LCO 3.0.6, the Distribution System's ACTIONS are not entered even if all AC sources to it are inoperable, resulting in de-energization. Therefore, the Required Actions of Condition A are modified by a Note to indicate that when Condition A is entered with no AC power to any required ESF bus, the ACTIONS for LCO 3.8.10 must be immediately entered. This Note allows Condition A to provide requirements for the loss of the offsite circuit, whether or not a train is de-energized. LCO 3.8.10 provides the appropriate restrictions for the situation involving a de-energized train.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.8.2.1

SR 3.8.2.1 requires the SRs from LCO 3.8.1 that are necessary for ensuring the OPERABILITY of the AC sources in other than MODES 1, 2, 3, and 4. SR 3.8.1.8 is not required to be met since only one offsite circuit is required to be OPERABLE. SR 3.8.1.12 and SR 3.8.1.19 are not required to be met because the ESF actuation signal is not required to be OPERABLE. SR 3.8.1.17 is not required to be met because the required OPERABLE DG(s) is not required to undergo periods of being synchronized to the offsite circuit. SR 3.8.1.20 is excepted because starting independence is not required with DG(s) that are not required to be OPERABLE.

This SR is modified by a Note. The reason for the Note is to preclude requiring the OPERABLE DG(s) from being paralleled with the offsite power network or otherwise rendered inoperable during performance of SRs, and to preclude deenergizing a required 4160 V ESF bus or disconnecting a required offsite circuit during performance of SRs. With limited AC Sources available, a single event could compromise both the required circuit and the DG. It is the intent that these SRs must still be capable of being met, but actual performance is not required during periods when the DG and offsite circuit is required to be OPERABLE. Refer to the corresponding Bases for LCO 3.8.1 for a discussion of each SR.

REFERENCES

None.

B 3.8 ELECTRICAL POWER SYSTEMS

B 3.8.3 Diesel Fuel Oil, Lube Oil, and Starting Air

BASES

BACKGROUND

Each diesel generator (DG) is provided with a storage tank having a fuel oil capacity sufficient to operate that diesel for a period of 7 days, while the DG is supplying maximum post loss of coolant accident load demand as discussed in the FSAR, Section [9.5.4.2] (Ref. 1). The maximum load demand is calculated using the assumption that at least two DGs are available. This onsite fuel oil capacity is sufficient to operate the DGs for longer than the time to replenish the onsite supply from outside sources.

Fuel oil is transferred from storage tank to day tank by either of two transfer pumps associated with each storage tank. Redundancy of pumps and piping precludes the failure of one pump, or the rupture of any pipe, valve, or tank to result in the loss of more than one DG. All outside tanks, pumps, and piping are located underground.

For proper operation of the standby DGs, it is necessary to ensure the proper quality of the fuel oil. Regulatory Guide 1.137 (Ref. 2) addresses the recommended fuel oil practices as supplemented by ANSI N195-1976 (Ref. 3). The fuel oil properties governed by these SRs are the water and sediment content, the kinematic viscosity, specific gravity (or API gravity), and impurity level.

The DG lubrication system is designed to provide sufficient lubrication to permit proper operation of its associated DG under all loading conditions. The system is required to circulate the lube oil to the diesel engine working surfaces and to remove excess heat generated by friction during operation. Each engine oil sump contains an inventory capable of supporting a minimum of [7] days of operation. [The onsite storage in addition to the engine oil sump is sufficient to ensure 7 days of continuous operation.] This supply is sufficient supply to allow the operator to replenish lube oil from outside sources.

Each DG has an air start system with adequate capacity for five successive start attempts on the DG without recharging the air start receiver(s).

BASES

APPLICABLE SAFETY ANALYSES	The initial conditions of Design Basis Accident (DBA) and transient analyses in the FSAR, Chapter [6] (Ref. 4), and in the FSAR, Chapter [15] (Ref. 5), assume Engineered Safety Feature (ESF) systems are OPERABLE. The DGs are designed to provide sufficient capacity, capability, redundancy, and reliability to ensure the availability of necessary power to ESF systems so that fuel, Reactor Coolant System and containment design limits are not exceeded. These limits are discussed in more detail in the Bases for LCO Section 3.2, Power Distribution Limits; Section 3.4, Reactor Coolant System (RCS); and Section 3.6, Containment Systems. Since diesel fuel oil, lube oil, and the air start subsystems support the operation of the standby AC power sources, they satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).
LCO	Stored diesel fuel oil is required to have sufficient supply for 7 days of full load operation. It is also required to meet specific standards for quality. Additionally, sufficient lubricating oil supply must be available to ensure the capability to operate at full load for 7 days. This requirement, in conjunction with an ability to obtain replacement supplies within 7 days, supports the availability of DGs required to shut down the reactor and to maintain it in a safe condition for an anticipated operational occurrence (AOO) or a postulated DBA with loss of offsite power. DG day tank fuel requirements, as well as transfer capability from the storage tank to the day tank, are addressed in LCO 3.8.1, "AC Sources - Operating," and LCO 3.8.2, "AC Sources - Shutdown." The starting air system is required to have a minimum capacity for five successive DG start attempts without recharging the air start receivers.
APPLICABILITY	The AC sources (LCO 3.8.1 and LCO 3.8.2) are required to ensure the availability of the required power to shut down the reactor and maintain it in a safe shutdown condition after an AOO or a postulated DBA. Since stored diesel fuel oil, lube oil, and starting air subsystems support LCO 3.8.1 and LCO 3.8.2, stored diesel fuel oil, lube oil and starting air are required to be within limits when the associated DG is required to be OPERABLE.
ACTIONS	The ACTIONS Table is modified by a Note indicating that separate Condition entry is allowed for each DG. This is acceptable, since the Required Actions for each Condition provide appropriate compensatory actions for each inoperable DG subsystem. Complying with the Required Actions for one inoperable DG subsystem may allow for continued operation, and subsequent inoperable DG subsystem(s) are governed by separate Condition entry and application of associated Required Actions.

BASES

ACTIONS (continued)

A.1

In this Condition, the 7 day fuel oil supply for a DG is not available. However, the Condition is restricted to fuel oil level reductions, that maintain at least a 6 day supply. These circumstances may be caused by events such as full load operation required after an inadvertent start while at minimum required level; or feed and bleed operations, which may be necessitated by increasing particulate levels or any number of other oil quality degradations. This restriction allows sufficient time for obtaining the requisite replacement volume and performing the analyses required prior to addition of fuel oil to the tank. A period of 48 hours is considered sufficient to complete restoration of the required level prior to declaring the DG inoperable. This period is acceptable based on the remaining capacity (≥ 6 days), the fact that procedures will be initiated to obtain replenishment, and the low probability of an event during this brief period.

B.1

With lube oil inventory < 500 gal, sufficient lubricating oil to support 7 days of continuous DG operation at full load conditions may not be available. However, the Condition is restricted to lube oil volume reductions that maintain at least a 6 day supply. This restriction allows sufficient time to obtain the requisite replacement volume. A period of 48 hours is considered sufficient to complete restoration of the required volume prior to declaring the DG inoperable. This period is acceptable based on the remaining capacity (> 6 days), the low rate of usage, the fact that procedures will be initiated to obtain replenishment, and the low probability of an event during this brief period.

C.1

This Condition is entered as a result of a failure to meet the acceptance criterion of SR 3.8.3.5. Normally, trending of particulate levels allows sufficient time to correct high particulate levels prior to reaching the limit of acceptability. Poor sample procedures (bottom sampling), contaminated sampling equipment, and errors in laboratory analysis can produce failures that do not follow a trend. Since the presence of particulates does not mean failure of the fuel oil to burn properly in the diesel engine, and particulate concentration is unlikely to change

BASES

ACTIONS (continued)

significantly between Surveillance Frequency intervals, and proper engine performance has been recently demonstrated (within 31 days), it is prudent to allow a brief period prior to declaring the associated DG inoperable. The 7 day Completion Time allows for further evaluation, resampling, and re-analysis of the DG fuel oil.

D.1

With the new fuel oil properties defined in the Bases for SR 3.8.3.4 not within the required limits, a period of 30 days is allowed for restoring the stored fuel oil properties. This period provides sufficient time to test the stored fuel oil to determine that the new fuel oil, when mixed with previously stored fuel oil, remains acceptable, or restore the stored fuel oil properties. This restoration may involve feed and bleed procedures, filtering, or combinations of these procedures. Even if a DG start and load was required during this time interval and the fuel oil properties were outside limits, there is a high likelihood that the DG would still be capable of performing its intended function.

E.1

With starting air receiver pressure < [225] psig, sufficient capacity for five successive DG start attempts does not exist. However, as long as the receiver pressure is > [125] psig, there is adequate capacity for at least one start attempt, and the DG can be considered OPERABLE while the air receiver pressure is restored to the required limit. A period of 48 hours is considered sufficient to complete restoration to the required pressure prior to declaring the DG inoperable. This period is acceptable based on the remaining air start capacity, the fact that most DG starts are accomplished on the first attempt, and the low probability of an event during this brief period.

F.1

With a Required Action and associated Completion Time not met, or one or more DGs with diesel fuel oil, lube oil, or starting air subsystem not within limits for reasons other than addressed by Conditions A through E, the associated DG may be incapable of performing its intended function and must be immediately declared inoperable.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.8.3.1

This SR provides verification that there is an adequate inventory of fuel oil in the storage tanks to support each DG's operation for 7 days at full load. The 7 day period is sufficient time to place the unit in a safe shutdown condition and to bring in replenishment fuel from an offsite location.

The 31 day Frequency is adequate to ensure that a sufficient supply of fuel oil is available, since low level alarms are provided and unit operators would be aware of any large uses of fuel oil during this period.

SR 3.8.3.2

This Surveillance ensures that sufficient lube oil inventory is available to support at least 7 days of full load operation for each DG. The [500] gal requirement is based on the DG manufacturer consumption values for the run time of the DG. Implicit in this SR is the requirement to verify the capability to transfer the lube oil from its storage location to the DG, when the DG lube oil sump does not hold adequate inventory for 7 days of full load operation without the level reaching the manufacturer recommended minimum level.

A 31 day Frequency is adequate to ensure that a sufficient lube oil supply is onsite, since DG starts and run time are closely monitored by the unit staff.

SR 3.8.3.3

The tests listed below are a means of determining whether new fuel oil is of the appropriate grade and has not been contaminated with substances that would have an immediate, detrimental impact on diesel engine combustion. If results from these tests are within acceptable limits, the fuel oil may be added to the storage tanks without concern for contaminating the entire volume of fuel oil in the storage tanks. These tests are to be conducted prior to adding the new fuel to the storage tank(s), but in no case is the time between receipt of new fuel and conducting the tests to exceed 31 days. The tests, limits, and applicable ASTM Standards are as follows:

a. Sample the new fuel oil in accordance with ASTM D4057-[ ] (Ref. 6),

BASES

SURVEILLANCE REQUIREMENTS (continued)

b. Verify in accordance with the tests specified in ASTM D975-[ ] (Ref. 6) that the sample has an absolute specific gravity at 60/60°F of ≥ 0.83 and ≤ 0.89, or an API gravity at 60°F of ≥ 27° and ≤ 39° when tested in accordance with ASTM D1298-[ ] (Ref. 6), a kinematic viscosity at 40°C of ≥ 1.9 centistokes and ≤ 4.1 centistokes, and a flash point ≥ 125°F, and

c. Verify that the new fuel oil has a clear and bright appearance with proper color when tested in accordance with ASTM D4176-[ ] or a water and sediment content within limits when tested in accordance with [ASTM D2709-[ ]] (Ref. 6).

Failure to meet any of the above limits is cause for rejecting the new fuel oil, but does not represent a failure to meet the LCO concern since the fuel oil is not added to the storage tanks.

Within 31 days following the initial new fuel oil sample, the fuel oil is analyzed to establish that the other properties specified in Table 1 of ASTM D975-[ ] (Ref. 7) are met for new fuel oil when tested in accordance with ASTM D975-[ ] (Ref. 6), except that the analysis for sulfur may be performed in accordance with ASTM D1552-[ ], ASTM D2622-[ ], or ASTM D4294-[ ] (Ref. 6). The 31 day period is acceptable because the fuel oil properties of interest, even if they were not within stated limits, would not have an immediate effect on DG operation. This Surveillance ensures the availability of high quality fuel oil for the DGs.

Fuel oil degradation during long term storage shows up as an increase in particulate, due mostly to oxidation. The presence of particulate does not mean the fuel oil will not burn properly in a diesel engine. The particulate can cause fouling of filters and fuel oil injection equipment, however, which can cause engine failure.

Particulate concentrations should be determined in accordance with ASTM D5452-[ ] (Ref. 6). This method involves a gravimetric determination of total particulate concentration in the fuel oil and has a limit of 10 mg/l. It is acceptable to obtain a field sample for subsequent laboratory testing in lieu of field testing. [For those designs in which the total stored fuel oil volume is contained in two or more interconnected tanks, each tank must be considered and tested separately.]

The Frequency of this test takes into consideration fuel oil degradation trends that indicate that particulate concentration is unlikely to change significantly between Frequency intervals.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.8.3.4

This Surveillance ensures that, without the aid of the refill compressor, sufficient air start capacity for each DG is available. The system design requirements provide for a minimum of [five] engine start cycles without recharging. [A start cycle is defined by the DG vendor, but usually is measured in terms of time (seconds or cranking) or engine cranking speed.] The pressure specified in this SR is intended to reflect the lowest value at which the [five] starts can be accomplished.

The 31 day Frequency takes into account the capacity, capability, redundancy, and diversity of the AC sources and other indications available in the control room, including alarms, to alert the operator to below normal air start pressure.

SR 3.8.3.5

Microbiological fouling is a major cause of fuel oil degradation. There are numerous bacteria that can grow in fuel oil and cause fouling, but all must have a water environment in order to survive. Removal of water from the fuel storage tanks once every [31] days eliminates the necessary environment for bacterial survival. This is the most effective means of controlling microbiological fouling. In addition, it eliminates the potential for water entrainment in the fuel oil during DG operation. Water may come from any of several sources, including condensation, ground water, rain water, and contaminated fuel oil, and from breakdown of the fuel oil by bacteria. Frequent checking for and removal of accumulated water minimizes fouling and provides data regarding the watertight integrity of the fuel oil system. The Surveillance Frequencies are established by Regulatory Guide 1.137 (Ref. 2). This SR is for preventative maintenance. The presence of water does not necessarily represent failure of this SR provided the accumulated water is removed during performance of the Surveillance.

REFERENCES

1. FSAR, Section [9.5.4.2].

2. Regulatory Guide 1.137.

3. ANSI N195-1976, Appendix B.

4. FSAR, Chapter [6].

BASES

REFERENCES (continued)

5. FSAR, Chapter [15].

6. ASTM Standards: D4057-[ ]; D975-[ ]; D1298-[ ]; D4176-[ ]; [D2709-[ ];] D1552-[ ]; D2622-[ ]; D4294-[ ]; D5452-[ ].

7. ASTM Standards, D975-[ ], Table 1.

B 3.8 ELECTRICAL POWER SYSTEMS

B 3.8.4 DC Sources - Operating

BASES

BACKGROUND

The station DC electrical power system provides the AC emergency power system with control power. It also provides both motive and control power to selected safety related equipment and preferred AC vital bus power (via inverters). As required by 10 CFR 50, Appendix A, GDC 17 (Ref. 1), the DC electrical power system is designed to have sufficient independence, redundancy, and testability to perform its safety functions, assuming a single failure. The DC electrical power system also conforms to the recommendations of Regulatory Guide 1.6 (Ref. 2) and IEEE-308 (Ref. 3).

The [125/250] VDC electrical power system consists of two independent and redundant safety related Class 1E DC electrical power subsystems ([Train A and Train B]). Each subsystem consists of [two] 125 VDC batteries [(each battery [50]% capacity)], the associated battery charger(s) for each battery, and all the associated control equipment and interconnecting cabling.

[The 250 VDC source is obtained by use of the two 125 VDC batteries connected in series. Additionally there is [one] spare battery charger per subsystem, which provides backup service in the event that the preferred battery charger is out of service. If the spare battery charger is substituted for one of the preferred battery chargers, then the requirements of independence and redundancy between subsystems are maintained.]

During normal operation, the [125/250] VDC load is powered from the battery chargers with the batteries floating on the system. In case of loss of normal power to the battery charger, the DC load is automatically powered from the station batteries.

The [Train A and Train B] DC electrical power subsystems provide the control power for its associated Class 1E AC power load group, [4.16] kV switchgear, and [480] V load centers. The DC electrical power subsystems also provide DC electrical power to the inverters, which in turn power the AC vital buses.

The DC power distribution system is described in more detail in the Bases for LCO 3.8.9, "Distributions System Operating," and for LCO 3.8.10, "Distribution Systems - Shutdown."

BASES

BACKGROUND (continued)

Each 125/250 VDC battery is separately housed in a ventilated room apart from its charger and distribution centers. Each subsystem is located in an area separated physically and electrically from the other subsystem to ensure that a single failure in one subsystem does not cause a failure in a redundant subsystem. There is no sharing between redundant Class 1E subsystems, such as batteries, battery chargers, or distribution panels.

Each battery has adequate storage capacity to meet the duty cycle(s) discussed in the FSAR, Chapter [8] (Ref 4). The battery is designed with additional capacity above that required by the design duty cycle to allow for temperature variations and other factors.

The batteries for Train A and Train B DC electrical power subsystems are sized to produce required capacity at 80% of nameplate rating, corresponding to warranted capacity at end of life cycles and the 100% design demand. The minimum design voltage limit is 105/210 V.

The battery cells are of flooded lead acid construction with a nominal specific gravity of [1.215]. This specific gravity corresponds to an open circuit battery voltage of approximately 120 V for a [58] cell battery (i.e., cell voltage of [2.065] volts per cell (Vpc)). The open circuit voltage is the voltage maintained when there is no charging or discharging. Once fully charged with its open circuit voltage ≥ [2.065] Vpc, the battery cell will maintain its capacity for [30] days without further charging per manufacturer's instructions. Optimal long term performance however, is obtained by maintaining a float voltage [2.20 to 2.25] Vpc. This provides adequate over-potential, which limits the formation of lead sulfate and self discharge. The nominal float voltage of [2.22] Vpc corresponds to a total float voltage output of [128.8] V for a [58] cell battery as discussed in the FSAR, Chapter [8] (Ref. 4).

Each Train A and Train B DC electrical power subsystem battery charger has ample power output capacity for the steady state operation of connected loads required during normal operation, while at the same time maintaining its battery bank fully charged. Each battery charger also has sufficient excess capacity to restore the battery from the design minimum charge to its fully charged state within 24 hours while supplying normal steady state loads discussed in the FSAR, Chapter [8] (Ref. 4).

BASES

BACKGROUND (continued)

The battery charger is normally in the float-charge mode. Float-charge is the condition in which the charger is supplying the connected loads and the battery cells are receiving adequate current to optimally charge the battery. This assures the internal losses of a battery are overcome and the battery is maintained in a fully charged state.

When desired, the charger can be placed in the equalize mode. The equalize mode is at a higher voltage than the float mode and charging current is correspondingly higher. The battery charger is operated in the equalize mode after a battery discharge or for routine maintenance. Following a battery discharge, the battery recharge characteristic accepts current at the current limit of the battery charger (if the discharge was significant, e.g., following a battery service test) until the battery terminal voltage approaches the charger voltage setpoint. Charging current then reduces exponentially during the remainder of the recharge cycle. Lead-calcium batteries have recharge efficiencies of greater than 95%, so once at least 105% of the ampere-hours discharged have been returned, the battery capacity would be restored to the same condition as it was prior to the discharge. This can be monitored by direct observation of the exponentially decaying charging current or by evaluating the amp-hours discharged from the battery and amp-hours returned to the battery.

APPLICABLE SAFETY ANALYSES

The initial conditions of Design Basis Accident (DBA) and transient analyses in the FSAR, Chapter [6] (Ref. 5) and Chapter [15] (Ref. 6), assume that Engineered Safety Feature (ESF) systems are OPERABLE. The DC electrical power system provides normal and emergency DC electrical power for the DGs, emergency auxiliaries, and control and switching during all MODES of operation.

The OPERABILITY of the DC sources is consistent with the initial assumptions of the accident analyses and is based upon meeting the design basis of the unit. This includes maintaining the DC sources OPERABLE during accident conditions in the event of:

a. An assumed loss of all offsite AC power or all onsite AC power and

b. A worst-case single failure.

The DC sources satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO

The DC electrical power subsystems, each subsystem consisting of [two] batteries, battery charger [for each battery] and the corresponding control equipment and interconnecting cabling supplying power to the associated bus within the train are required to be OPERABLE to ensure the availability of the required power to shut down the reactor and maintain it in a safe condition after an anticipated operational occurrence (AOO) or a postulated DBA. Loss of any train DC electrical power subsystem does not prevent the minimum safety function from being performed (Ref. 4).

An OPERABLE DC electrical power subsystem requires all required batteries and respective chargers to be operating and connected to the associated DC bus(es).

APPLICABILITY

The DC electrical power sources are required to be OPERABLE in MODES 1, 2, 3, and 4 to ensure safe unit operation and to ensure that:

a. Acceptable fuel design limits and reactor coolant pressure boundary limits are not exceeded as a result of AOOs or abnormal transients and

b. Adequate core cooling is provided, and containment integrity and other vital functions are maintained in the event of a postulated DBA.

The DC electrical power requirements for MODES 5 and 6 are addressed in the Bases for LCO 3.8.5, "DC Sources - Shutdown."

ACTIONS

A.1, A.2, and A.3

Condition A represents one train with one [or two] battery chargers inoperable (e.g., the voltage limit of SR 3.8.4.1 is not maintained). The ACTIONS provide a tiered response that focuses on returning the battery to the fully charged state and restoring a fully qualified charger to OPERABLE status in a reasonable time period. Required Action A.1 requires that the battery terminal voltage be restored to greater than or equal to the minimum established float voltage within 2 hours. This time provides for returning the inoperable charger to OPERABLE status or providing an alternate means of restoring battery terminal voltage to greater than or equal to the minimum established float voltage. Restoring the battery terminal voltage to greater than or equal to the minimum established float voltage provides good assurance that, within [12] hours, the battery will be restored to its fully charged condition (Required Action A.2) from any discharge that might have occurred due to the charger inoperability.

BASES

ACTIONS (continued)

-----------------------------------REVIEWER'S NOTE-----------------------------------
A plant that cannot meet the 12 hour Completion Time due to an inherent battery charging characteristic can propose an alternate time equal to 2 hours plus the time experienced to accomplish the exponential charging current portion of the battery charge profile following the service test (SR 3.8.4.3).

A discharged battery having terminal voltage of at least the minimum established float voltage indicates that the battery is on the exponential charging current portion (the second part) of its recharge cycle. The time to return a battery to its fully charged state under this condition is simply a function of the amount of the previous discharge and the recharge characteristic of the battery. Thus there is good assurance of fully recharging the battery within [12] hours, avoiding a premature shutdown with its own attendant risk.

If established battery terminal float voltage cannot be restored to greater than or equal to the minimum established float voltage within 2 hours, and the charger is not operating in the current-limiting mode, a faulty charger is indicated. A faulty charger that is incapable of maintaining established battery terminal float voltage does not provide assurance that it can revert to and operate properly in the current limit mode that is necessary during the recovery period following a battery discharge event that the DC system is designed for.

If the charger is operating in the current limit mode after 2 hours that is an indication that the battery is partially discharged and its capacity margins will be reduced. The time to return the battery to its fully charged condition in this case is a function of the battery charger capacity, the amount of loads on the associated DC system, the amount of the previous discharge, and the recharge characteristic of the battery. The charge time can be extensive, and there is not adequate assurance that it can be recharged within [12] hours (Required Action A.2).

Required Action A.2 requires that the battery float current be verified as less than or equal to [2] amps. This indicates that, if the battery had been discharged as the result of the inoperable battery charger, it has now been fully recharged. If at the expiration of the initial [12] hour period the battery float current is not less than or equal to [2] amps this indicates there may be additional battery problems and the battery must be declared inoperable.

BASES

ACTIONS (continued)

Required Action A.3 limits the restoration time for the inoperable battery charger to 7 days. This action is applicable if an alternate means of restoring battery terminal voltage to greater than or equal to the minimum established float voltage has been used (e.g., balance of plant non-Class 1E battery charger). The 7 day Completion Time reflects a reasonable time to effect restoration of the qualified battery charger to OPERABLE status.

B.1

----------------------------------REVIEWER'S NOTE----------------------------------
The 2 hour Completion Times of Required Actions B.1 and C.1 are in brackets. Any licensee wishing to request a longer Completion Time will need to demonstrate that the longer Completion Time is appropriate for the plant in accordance with the guidance in Regulatory Guide (RG) 1.177, "An Approach for Plant-Specific, Risk-Informed Decision Making: Technical Specifications."

Condition B represents one train with one [or two] batter[y][ies] inoperable. With one [or two] batter[y][ies] inoperable, the DC bus is being supplied by the OPERABLE battery charger[s]. Any event that results in a loss of the AC bus supporting the battery charger[s] will also result in loss of DC to that train. Recovery of the AC bus, especially if it is due to a loss of offsite power, will be hampered by the fact that many of the components necessary for the recovery (e.g., diesel generator control and field flash, AC load shed and diesel generator output circuit breakers, etc.) likely rely upon the batter[y][ies]. In addition the energization transients of any DC loads that are beyond the capability of the battery charger[s] and normally require the assistance of the batter[y][ies] will not be able to be brought online. The [2] hour limit allows sufficient time to effect restoration of an inoperable battery given that the majority of the conditions that lead to battery inoperability (e.g., loss of battery charger, battery cell voltage less than [2.07] V, etc.) are identified in Specifications 3.8.4, 3.8.5, and 3.8.6 together with additional specific completion times.

BASES

ACTIONS (continued)

C.1

Condition C represents one train with a loss of ability to completely respond to an event, and a potential loss of ability to remain energized during normal operation. It is therefore, imperative that the operator's attention focus on stabilizing the unit, minimizing the potential for complete loss of DC power to the affected train. The 2 hour limit is consistent with the allowed time for an inoperable DC distribution system train.

If one of the required DC electrical power subsystems is inoperable for reasons other than Condition A or B (e.g., inoperable battery charger and associated inoperable battery), the remaining DC electrical power subsystem has the capacity to support a safe shutdown and to mitigate an accident condition. Since a subsequent worst case single failure could, however, result in the loss of minimum necessary DC electrical subsystems to mitigate a worst case accident, continued power operation should not exceed 2 hours. The 2 hour Completion Time is based on Regulatory Guide 1.93 (Ref. 7) and reflects a reasonable time to assess unit status as a function of the inoperable DC electrical power subsystem and, if the DC electrical power subsystem is not restored to OPERABLE status, to prepare to effect an orderly and safe unit shutdown.

D.1 and D.2

If the inoperable DC electrical power subsystem cannot be restored to OPERABLE status within the required Completion Time, the unit must be brought to a MODE in which the LCO does not apply. To achieve this status, the unit must be brought to at least MODE 3 within 6 hours and to MODE 5 within 36 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required unit conditions from full power conditions in an orderly manner and without challenging plant systems. The Completion Time to bring the unit to MODE 5 is consistent with the time required in Regulatory Guide 1.93 (Ref. 7).

SURVEILLANCE REQUIREMENTS

SR 3.8.4.1

Verifying battery terminal voltage while on float charge helps to ensure the effectiveness of the battery chargers, which support the ability of the batteries to perform their intended function. Float charge is the condition in which the charger is supplying the continuous charge required to overcome the internal losses of a battery and maintain the battery in a

BASES

SURVEILLANCE REQUIREMENTS (continued)

fully charged state while supplying the continuous steady state loads of the associated DC subsystem. On float charge, battery cells will receive adequate current to optimally charge the battery. The voltage requirements are based on the nominal design voltage of the battery and are consistent with the minimum float voltage established by the battery manufacturer ([2.20] Vpc or [127.6] V at the battery terminals). This voltage maintains the battery plates in a condition that supports maintaining the grid life (expected to be approximately 20 years). The 7 day Frequency is consistent with manufacturer recommendations and IEEE-450 (Ref. 8).

SR 3.8.4.2

This SR verifies the design capacity of the battery chargers. According to Regulatory Guide 1.32 (Ref. 9), the battery charger supply is recommended to be based on the largest combined demands of the various steady state loads and the charging capacity to restore the battery from the design minimum charge state to the fully charged state, irrespective of the status of the unit during these demand occurrences. The minimum required amperes and duration ensure that these requirements can be satisfied.

This SR provides two options. One option requires that each battery charger be capable of supplying [400] amps at the minimum established float voltage for [8] hours. The ampere requirements are based on the output rating of the chargers. The voltage requirements are based on the charger voltage level after a response to a loss of AC power. The time period is sufficient for the charger temperature to have stabilized and to have been maintained for at least [2] hours.

The other option requires that each battery charger be capable of recharging the battery after a service test coincident with supplying the largest coincident demands of the various continuous steady state loads (irrespective of the status of the plant during which these demands occur). This level of loading may not normally be available following the battery service test and will need to be supplemented with additional loads. The duration for this test may be longer than the charger sizing criteria since the battery recharge is affected by float voltage, temperature, and the exponential decay in charging current. The battery is recharged when the measured charging current is ≤ [2] amps.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The Surveillance Frequency is acceptable, given the unit conditions required to perform the test and the other administrative controls existing to ensure adequate charger performance during these [18 month] intervals. In addition, this Frequency is intended to be consistent with expected fuel cycle lengths.

SR 3.8.4.3

A battery service test is a special test of the battery capability, as found, to satisfy the design requirements (battery duty cycle) of the DC electrical power system. The discharge rate and test length should correspond to the design duty cycle requirements as specified in Reference 4.

The Surveillance Frequency of [18 months] is consistent with the recommendations of Regulatory Guide 1.32 (Ref. 9) and Regulatory Guide 1.129 (Ref. 10), which state that the battery service test should be performed during refueling operations, or at some other outage, with intervals between tests not to exceed [18 months].

This SR is modified by two Notes. Note 1 allows the performance of a modified performance discharge test in lieu of a service test.

The reason for Note 2 is that performing the Surveillance would perturb the electrical distribution system and challenge safety systems. This restriction from normally performing the Surveillance in MODE 1 or 2 is further amplified to allow portions of the Surveillance to be performed for the purpose of reestablishing OPERABILITY (e.g., post work testing following corrective maintenance, corrective modification, deficient or incomplete surveillance testing, and other unanticipated OPERABILITY concerns) provided an assessment determines plant safety is maintained or enhanced. This assessment shall, as a minimum, consider the potential outcomes and transients associated with a failed partial Surveillance, a successful partial Surveillance, and a perturbation of the offsite or onsite system when they are tied together or operated independently for the partial Surveillance; as well as the operator procedures available to cope with these outcomes. These shall be measured against the avoided risk of a plant shutdown and startup to determine that plant safety is maintained or enhanced when portions of the Surveillance are performed in MODE 1 or 2. Risk insights or deterministic methods may be used for the assessment. Credit may be taken for unplanned events that satisfy this SR.

BASES

REFERENCES

1. 10 CFR 50, Appendix A, GDC 17.
2. Regulatory Guide 1.6, March 10, 1971.
3. IEEE-308-[1978].
4. FSAR, Chapter [8].
5. FSAR, Chapter [6].
6. FSAR, Chapter [15].
7. Regulatory Guide 1.93, December 1974.
8. IEEE-450-[1995].
9. Regulatory Guide 1.32, February 1977.
10. Regulatory Guide 1.129, December 1974.

B 3.8 ELECTRICAL POWER SYSTEMS

B 3.8.5 DC Sources - Shutdown

BASES

BACKGROUND	A description of the DC sources is provided in the Bases for LCO 3.8.4, "DC Sources - Operating."

APPLICABLE SAFETY ANALYSES

The initial conditions of Design Basis Accident (DBA) and transient analyses in the FSAR, Chapter [6] (Ref. 1) and Chapter [15] (Ref. 2), assume that Engineered Safety Feature (ESF) systems are OPERABLE. The DC electrical power system provides normal and emergency DC electrical power for the DGs, emergency auxiliaries, and control and switching during all MODES of operation.

The OPERABILITY of the DC subsystems is consistent with the initial assumptions of the accident analyses and the requirements for the supported systems' OPERABILITY.

The OPERABILITY of the minimum DC electrical power sources during MODES 5 and 6 and during movement of [recently] irradiated fuel assemblies ensures that:

a. The unit can be maintained in the shutdown or refueling condition for extended periods,

b. Sufficient instrumentation and control capability is available for monitoring and maintaining the unit status, and

c. Adequate DC electrical power is provided to mitigate events postulated during shutdown, such as a fuel handling accident [involving handling recently irradiated fuel. Due to radioactive decay, DC electrical power is only required to mitigate fuel handling accidents involving handling recently irradiated fuel (i.e., fuel that has occupied part of a critical reactor core within the previous [X] days)].

In general, when the unit is shut down, the Technical Specifications requirements ensure that the unit has the capability to mitigate the consequences of postulated accidents. However, assuming a single failure and concurrent loss of all offsite or all onsite power is not required. The rationale for this is based on the fact that many DBAs that are

BASES

APPLICABLE SAFETY ANALYSES (continued)

analyzed in MODES [1, 2, 3, and 4] have no specific analyses in MODES [5 and 6] because the energy contained within the reactor pressure boundary, reactor coolant temperature and pressure, and the corresponding stresses result in the probabilities of occurrence being significantly reduced or eliminated, and in minimal consequences. These deviations from DBA analysis assumptions and design requirements during shutdown conditions are allowed by the LCO for required systems.

The shutdown Technical Specification requirements are designed to ensure that the unit has the capability to mitigate the consequences of certain postulated accidents. Worst case DBAs which are analyzed for operating MODES are generally viewed not to be a significant concern during shutdown MODES due to the lower energies involved. The Technical Specifications therefore require a lesser complement of electrical equipment to be available during shutdown than is required during operating MODES. More recent work completed on the potential risks associated with shutdown, however, have found significant risk associated with certain shutdown evolutions. As a result, in addition to the requirements established in the Technical Specifications, the industry has adopted NUMARC 91-06, "Guidelines for Industry Actions to Assess Shutdown Management," as an Industry initiative to manage shutdown tasks and associated electrical support to maintain risk at an acceptable low level. This may require the availability of additional equipment beyond that required by the shutdown Technical Specifications.

The DC sources satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

The DC electrical power subsystems, [each required] [the required] subsystem consisting of two batteries, one battery charger per battery, and the corresponding control equipment and interconnecting cabling within the train, [are] [is] required to be OPERABLE to support [required] [one] train[s] of distribution systems required [OPERABLE by LCO 3.8.10, "Distribution Systems - Shutdown."] This ensures the availability of sufficient DC electrical power sources to operate the unit in a safe manner and to mitigate the consequences of postulated events during shutdown (e.g., fuel handling accidents [involving handling recently irradiated fuel]).

BASES

APPLICABILITY

The DC electrical power sources required to be OPERABLE in MODES 5 and 6, and during movement of [recently] irradiated fuel assemblies provide assurance that:

a. Required features needed to mitigate a fuel handling [involving handling recently irradiated fuel (i.e., fuel that has occupied part of a critical reactor core within the previous [X] days)] accident are available,

b. Required features necessary to mitigate the effects of events that can lead to core damage during shutdown are available, and

c. Instrumentation and control capability is available for monitoring and maintaining the unit in a cold shutdown condition or refueling condition.

The DC electrical power requirements for MODES 1, 2, 3, and 4 are covered in LCO 3.8.4.

ACTIONS

LCO 3.0.3 is not applicable while in MODE 5 or 6. However, since irradiated fuel assembly movement can occur in MODE 1, 2, 3, or 4, the ACTIONS have been modified by a Note stating that LCO 3.0.3 is not applicable. If moving irradiated fuel assemblies while in MODE 5 or 6, LCO 3.0.3 would not specify any action. If moving irradiated fuel assemblies while in MODE 1, 2, 3, or 4, the fuel movement is independent of reactor operations. Entering LCO 3.0.3, while in MODE 1, 2, 3, or 4 would require the unit to be shutdown unnecessarily.

<u>A.1, A.2, and A.3</u>

-----------------------------------REVIEWER'S NOTE-----------------------------------
ACTION A is included only when plant-specific implementation of LCO 3.8.5 includes the potential to require both trains of the DC System to be OPERABLE. If plant-specific implementation results in LCO 3.8.5 requiring only one train of the DC System to be OPERABLE, then ACTION A is omitted and ACTION B is renumbered as ACTION A.

Condition A represents one train with one [or two] battery chargers inoperable (e.g., the voltage limit of SR 3.8.4.1 is not maintained). The ACTIONS provide a tiered response that focuses on returning the battery to the fully charged state and restoring a fully qualified charger to OPERABLE status in a reasonable time period. Required Action A.1 requires that the battery terminal voltage be restored to greater than or

BASES

ACTIONS (continued)

equal to the minimum established float voltage within 2 hours. This time provides for returning the inoperable charger to OPERABLE status or providing an alternate means of restoring battery terminal voltage to greater than or equal to the minimum established float voltage. Restoring the battery terminal voltage to greater than or equal to the minimum established float voltage provides good assurance that, within [12] hours, the battery will be restored to its fully charged condition (Required Action A.2) from any discharge that might have occurred due to the charger inoperability.

-----------------------------------REVIEWER'S NOTE-----------------------------------
A plant that cannot meet the 12 hour Completion Time due to an inherent battery charging characteristic can propose an alternate time equal to 2 hours plus the time experienced to accomplish the exponential charging current portion of the battery charge profile following the service test (SR 3.8.4.3).

A discharged battery having terminal voltage of at least the minimum established float voltage indicates that the battery is on the exponential charging current portion (the second part) of its recharge cycle. The time to return a battery to its fully charged state under this condition is simply a function of the amount of the previous discharge and the recharge characteristic of the battery. Thus there is good assurance of fully recharging the battery within [12] hours, avoiding a premature shutdown with its own attendant risk.

If established battery terminal float voltage cannot be restored to greater than or equal to the minimum established float voltage within 2 hours, and the charger is not operating in the current-limiting modes, a faulty charger is indicated. A faulty charger that is incapable of maintaining established battery terminal float voltage does not provide assurance that it can revert to and operate properly in the current limit modes that is necessary during the recovery period following a battery discharge event that the DC system is designed for.

If the charger is operating in the current limit mode after 2 hours that is an indication that the battery is partially discharged and its capacity margins will be reduced. The time to return the battery to its fully charged condition in this case is a function of the battery charger capacity, the amount of loads on the associated DC system, the amount of the previous discharge, and the recharge characteristic of the battery. The charge time can be extensive, and there is not adequate assurance that it can be recharged within [12] hours (Required Action A.2).

BASES

ACTIONS (continued)

Required Action A.2 requires that the battery float current be verified as less than or equal to [2] amps. This indicates that, if the battery had been discharged as the result of the inoperable battery charger, it has now been fully recharged. If at the expiration of the initial [12] hour period the battery float current is not less than or equal to [2] amps this indicates there may be additional battery problems and the battery must be declared inoperable.

Required Action A.3 limits the restoration time for the inoperable battery charger to 7 days. This action is applicable if an alternate means of restoring battery terminal voltage to greater than or equal to the minimum established float voltage has been used (e.g., balance of plant non-Class 1E battery charger). The 7 day Completion Time reflects a reasonable time to effect restoration of the qualified battery charger to OPERABLE status.

<u>B.1, B.2.1, B.2.2, B.2.3, and B.2.4</u>

[If two trains are required by LCO 3.8.10, the remaining train with DC power available may be capable of supporting sufficient systems to allow continuation of CORE ALTERATIONS and [recently] irradiated fuel movement]. By allowing the option to declare required features inoperable with the associated DC power source(s) inoperable, appropriate restrictions will be implemented in accordance with the affected required features LCO ACTIONS. In many instances this option may involve undesired administrative efforts. Therefore, the allowance for sufficiently conservative actions is made (i.e., to suspend CORE ALTERATIONS, movement of [recently] irradiated fuel assemblies, and operations involving positive reactivity additions) that could result in loss of required SDM (MODE 5) or boron concentration (MODE 6). Suspending positive reactivity additions that could result in failure to meet the minimum SDM or boron concentration limit is required to assure continued safety operation. Introduction of coolant inventory must be from sources that have a boron concentration greater than that what would be required in the RCS for minimum SDM or refueling boron concentration. This may result in an overall reduction in RCS boron concentration, but provides acceptable margin to maintaining subcritical operation. Introduction of temperature changes including temperature increases when operating with a positive MTC must also be evaluated to ensure they do not result in a loss of required SDM.

BASES

ACTIONS (continued)

Suspension of these activities shall not preclude completion of actions to establish a safe conservative condition. These actions minimize probability of the occurrence of postulated events. It is further required to immediately initiate action to restore the required DC electrical power subsystem[s] and to continue this action until restoration is accomplished in order to provide the necessary DC electrical power to the unit safety systems.

The Completion Time of immediately is consistent with the required times for actions requiring prompt attention. The restoration of the required DC electrical power subsystems should be completed as quickly as possible in order to minimize the time during which the unit safety systems may be without sufficient power.

SURVEILLANCE REQUIREMENTS

SR 3.8.5.1

SR 3.8.5.1 states that Surveillances required by SR 3.8.4.1 through SR 3.8.4.3 are applicable in these MODES. See the corresponding Bases for LCO 3.8.4 for a discussion of each SR.

This SR is modified by a Note. The reason for the Note is to preclude requiring the OPERABLE DC sources from being discharged below their capability to provide the required power supply or otherwise rendered inoperable during the performance of SRs. It is the intent that these SRs must still be capable of being met, but actual performance is not required.

REFERENCES

1. FSAR, Chapter [6].

2. FSAR, Chapter [15].

B 3.8 ELECTRICAL POWER SYSTEMS

B 3.8.6 Battery Parameters

BASES

BACKGROUND

This LCO delineates the limits on battery float current as well as electrolyte temperature, level, and float voltage for the DC power subsystem batteries. A discussion of these batteries and their OPERABILITY requirements is provided in the Bases for LCO 3.8.4, "DC Sources - Operating," and LCO 3.8.5, "DC Sources - Shutdown." In addition to the limitations of this Specification, the [licensee controlled program] also implements a program specified in Specification 5.5.17 for monitoring various battery parameters that is based on the recommendations of IEEE Standard 450-1995, "IEEE Recommended Practice For Maintenance, Testing, And Replacement Of Vented Lead-Acid Batteries For Stationary Applications" (Ref. 1).

The battery cells are of flooded lead acid construction with a nominal specific gravity of [1.215]. This specific gravity corresponds to an open circuit battery voltage of approximately 120 V for [58] cell battery (i.e., cell voltage of [2.065] volts per cell (Vpc)). The open circuit voltage is the voltage maintained when there is no charging or discharging. Once fully charged with its open circuit voltage ≥ [2.065] Vpc, the battery cell will maintain its capacity for [30] days without further charging per manufacturer's instructions. Optimal long term performance however, is obtained by maintaining a float voltage [2.20 to 2.25] Vpc. This provides adequate over-potential which limits the formation of lead sulfate and self discharge. The nominal float voltage of [2.22] Vpc corresponds to a total float voltage output of [128.8] V for a [58] cell battery as discussed in the FSAR, Chapter [8] (Ref. 2).

APPLICABLE SAFETY ANALYSES

The initial conditions of Design Basis Accident (DBA) and transient analyses in the FSAR, Chapter [6] (Ref. 3) and Chapter [15] (Ref. 4), assume Engineered Safety Feature systems are OPERABLE. The DC electrical power system provides normal and emergency DC electrical power for the DGs, emergency auxiliaries, and control and switching during all MODES of operation.

The OPERABILITY of the DC subsystems is consistent with the initial assumptions of the accident analyses and is based upon meeting the design basis of the unit. This includes maintaining at least one train of DC sources OPERABLE during accident conditions, in the event of:

a. An assumed loss of all offsite AC power or all onsite AC power and

BASES

APPLICABLE SAFETY ANALYSES (continued)

b. A worst-case single failure.

Battery parameters satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

Battery parameters must remain within acceptable limits to ensure availability of the required DC power to shut down the reactor and maintain it in a safe condition after an anticipated operational occurrence or a postulated DBA. Battery parameter limits are conservatively established, allowing continued DC electrical system function even with limits not met. Additional preventative maintenance, testing, and monitoring performed in accordance with the [licensee controlled program] is conducted as specified in Specification 5.5.17.

APPLICABILITY

The battery parameters are required solely for the support of the associated DC electrical power subsystems. Therefore, battery parameter limits are only required when the DC power source is required to be OPERABLE. Refer to the Applicability discussion in Bases for LCO 3.8.4 and LCO 3.8.5.

ACTIONS

A.1, A.2, and A.3

With one or more cells in one or more batteries in one train < [2.07] V, the battery cell is degraded. Within 2 hours verification of the required battery charger OPERABILITY is made by monitoring the battery terminal voltage (SR 3.8.4.1) and of the overall battery state of charge by monitoring the battery float charge current (SR 3.8.6.1). This assures that there is still sufficient battery capacity to perform the intended function. Therefore, the affected battery is not required to be considered inoperable solely as a result of one or more cells in one or more batteries < [2.07] V, and continued operation is permitted for a limited period up to 24 hours.

Since the Required Actions only specify "perform," a failure of SR 3.8.4.1 or SR 3.8.6.1 acceptance criteria does not result in this Required Action not met. However, if one of the SRs is failed the appropriate Condition(s), depending on the cause of the failures, is entered. If SR 3.8.6.1 is failed then there is not assurance that there is still sufficient battery capacity to perform the intended function and the battery must be declared inoperable immediately.

BASES

ACTIONS (continued)

B.1 and B.2

One or more batteries in one train with float current > [2] amps indicates that a partial discharge of the battery capacity has occurred. This may be due to a temporary loss of a battery charger or possibly due to one or more battery cells in a low voltage condition reflecting some loss of capacity. Within 2 hours verification of the required battery charger OPERABILITY is made by monitoring the battery terminal voltage. If the terminal voltage is found to be less than the minimum established float voltage there are two possibilities, the battery charger is inoperable or is operating in the current limit mode. Condition A addresses charger inoperability. If the charger is operating in the current limit mode after 2 hours that is an indication that the battery has been substantially discharged and likely cannot perform its required design functions. The time to return the battery to its fully charged condition in this case is a function of the battery charger capacity, the amount of loads on the associated DC system, the amount of the previous discharge, and the recharge characteristic of the battery. The charge time can be extensive, and there is not adequate assurance that it can be recharged within [12] hours (Required Action B.2). The battery must therefore be declared inoperable.

If the float voltage is found to be satisfactory but there are one or more battery cells with float voltage less than [2.07] V, the associated "OR" statement in Condition F is applicable and the battery must be declared inoperable immediately. If float voltage is satisfactory and there are no cells less than [2.07] V there is good assurance that, within [12] hours, the battery will be restored to its fully charged condition (Required Action B.2) from any discharge that might have occurred due to a temporary loss of the battery charger.

----------------------------------REVIEWER'S NOTE----------------------------------
A plant that cannot meet the 12 hour Completion Time due to an inherent battery charging characteristic can propose an alternate time equal to 2 hours plus the time experienced to accomplish the exponential charging current portion of the battery charge profile following the service test (SR 3.8.4.3).

BASES

ACTIONS (continued)

A discharged battery with float voltage (the charger setpoint) across its terminals indicates that the battery is on the exponential charging current portion (the second part) of its recharge cycle. The time to return a battery to its fully charged state under this condition is simply a function of the amount of the previous discharge and the recharge characteristic of the battery. Thus there is good assurance of fully recharging the battery within [12] hours, avoiding a premature shutdown with its own attendant risk.

If the condition is due to one or more cells in a low voltage condition but still greater than [2.07] V and float voltage is found to be satisfactory, this is not indication of a substantially discharged battery and [12] hours is a reasonable time prior to declaring the battery inoperable.

Since Required Action B.1 only specifies "perform," a failure of SR 3.8.4.1 acceptance criteria does not result in the Required Action not met. However, if SR 3.8.4.1 is failed, the appropriate Condition(s), depending on the cause of the failure, is entered.

C.1, C.2, and C.3

With one or more batteries in one train with one or more cells electrolyte level above the top of the plates, but below the minimum established design limits, the battery still retains sufficient capacity to perform the intended function. Therefore, the affected battery is not required to be considered inoperable solely as a result of electrolyte level not met. Within 31 days the minimum established design limits for electrolyte level must be re-established.

With electrolyte level below the top of the plates there is a potential for dryout and plate degradation. Required Actions C.1 and C.2 address this potential (as well as provisions in Specification 5.5.17, Battery Monitoring and Maintenance Program). They are modified by a Note that indicates they are only applicable if electrolyte level is below the top of the plates. Within 8 hours level is required to be restored to above the top of the plates. The Required Action C.2 requirement to verify that there is no leakage by visual inspection and the Specification 5.5.17.b item to initiate action to equalize and test in accordance with manufacturer's recommendation are taken from Annex D of IEEE Standard 450-1995. They are performed following the restoration of the electrolyte level to above the top of the plates. Based on the results of the manufacturer's recommended testing the batter[y][ies] may have to be declared inoperable and the affected cell[s] replaced.

BASES

ACTIONS (continued)

D.1

With one or more batteries in one train with pilot cell temperature less than the minimum established design limits, 12 hours is allowed to restore the temperature to within limits. A low electrolyte temperature limits the current and power available. Since the battery is sized with margin, while battery capacity is degraded, sufficient capacity exists to perform the intended function and the affected battery is not required to be considered inoperable solely as a result of the pilot cell temperature not met.

E.1

With one or more batteries in redundant trains with battery parameters not within limits there is not sufficient assurance that battery capacity has not been affected to the degree that the batteries can still perform their required function, given that redundant batteries are involved. With redundant batteries involved this potential could result in a total loss of function on multiple systems that rely upon the batteries. The longer Completion Times specified for battery parameters on non-redundant batteries not within limits are therefore not appropriate, and the parameters must be restored to within limits on at least one train within 2 hours.

F.1

With one or more batteries with any battery parameter outside the allowances of the Required Actions for Condition A, B, C, D, or E, sufficient capacity to supply the maximum expected load requirement is not assured and the corresponding battery must be declared inoperable. Additionally, discovering one or more batteries in one train with one or more battery cells float voltage less than [2.07] V and float current greater than [2] amps indicates that the battery capacity may not be sufficient to perform the intended functions. The battery must therefore be declared inoperable immediately.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.8.6.1

Verifying battery float current while on float charge is used to determine the state of charge of the battery. Float charge is the condition in which the charger is supplying the continuous charge required to overcome the internal losses of a battery and maintain the battery in a charged state. The float current requirements are based on the float current indicative of a charged battery. Use of float current to determine the state of charge of the battery is consistent with IEEE-450 (Ref. 1). The 7 day Frequency is consistent with IEEE-450 (Ref. 1).

This SR is modified by a Note that states the float current requirement is not required to be met when battery terminal voltage is less than the minimum established float voltage of SR 3.8.4.1. When this float voltage is not maintained the Required Actions of LCO 3.8.4 ACTION A are being taken, which provide the necessary and appropriate verifications of the battery condition. Furthermore, the float current limit of [2] amps is established based on the nominal float voltage value and is not directly applicable when this voltage is not maintained.

SR 3.8.6.2 and SR 3.8.6.5

Optimal long term battery performance is obtained by maintaining a float voltage greater than or equal to the minimum established design limits provided by the battery manufacturer, which corresponds to [130.5] V at the battery terminals, or [2.25] Vpc. This provides adequate over-potential, which limits the formation of lead sulfate and self discharge, which could eventually render the battery inoperable. Float voltages in this range or less, but greater than [2.07] Vpc, are addressed in Specification 5.5.17. SRs 3.8.6.2 and 3.8.6.5 require verification that the cell float voltages are equal to or greater than the short term absolute minimum voltage of [2.07] V. The Frequency for cell voltage verification every 31 days for pilot cell and 92 days for each connected cell is consistent with IEEE-450 (Ref. 1).

SR 3.8.6.3

The limit specified for electrolyte level ensures that the plates suffer no physical damage and maintains adequate electron transfer capability. The Frequency is consistent with IEEE-450 (Ref. 1).

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.8.6.4

This Surveillance verifies that the pilot cell temperature is greater than or equal to the minimum established design limit (i.e., [40]°F). Pilot cell electrolyte temperature is maintained above this temperature to assure the battery can provide the required current and voltage to meet the design requirements. Temperatures lower than assumed in battery sizing calculations act to inhibit or reduce battery capacity. The Frequency is consistent with IEEE-450 (Ref. 1).

SR 3.8.6.6

A battery performance discharge test is a test of constant current capacity of a battery, normally done in the as found condition, after having been in service, to detect any change in the capacity determined by the acceptance test. The test is intended to determine overall battery degradation due to age and usage.

Either the battery performance discharge test or the modified performance discharge test is acceptable for satisfying SR 3.8.6.6; however, only the modified performance discharge test may be used to satisfy the battery service test requirements of SR 3.8.4.3.

A modified discharge test is a test of the battery capacity and its ability to provide a high rate, short duration load (usually the highest rate of the duty cycle). This will often confirm the battery's ability to meet the critical period of the load duty cycle, in addition to determining its percentage of rated capacity. Initial conditions for the modified performance discharge test should be identical to those specified for a service test.

It may consist of just two rates; for instance the one minute rate for the battery or the largest current load of the duty cycle, followed by the test rate employed for the performance test, both of which envelope the duty cycle of the service test. Since the ampere-hours removed by a one minute discharge represents a very small portion of the battery capacity, the test rate can be changed to that for the performance test without compromising the results of the performance discharge test. The battery terminal voltage for the modified performance discharge test must remain above the minimum battery terminal voltage specified in the battery service test for the duration of time equal to that of the service test.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The acceptance criteria for this Surveillance are consistent with IEEE-450 (Ref. 1) and IEEE-485 (Ref. 5). These references recommend that the battery be replaced if its capacity is below 80% of the manufacturer's rating. A capacity of 80% shows that the battery rate of deterioration is increasing, even if there is ample capacity to meet the load requirements. Furthermore, the battery is sized to meet the assumed duty cycle loads when the battery design capacity reaches this [80]% limit.

The Surveillance Frequency for this test is normally 60 months. If the battery shows degradation, or if the battery has reached 85% of its expected life and capacity is < 100% of the manufacturer's rating, the Surveillance Frequency is reduced to 12 months. However, if the battery shows no degradation but has reached 85% of its expected life, the Surveillance Frequency is only reduced to 24 months for batteries that retain capacity ≥ 100% of the manufacturer's ratings. Degradation is indicated, according to IEEE-450 (Ref. 1), when the battery capacity drops by more than 10% relative to its capacity on the previous performance test or when it is ≥ [10%] below the manufacturer's rating. These Frequencies are consistent with the recommendations in IEEE-450 (Ref. 1).

This SR is modified by a Note. The reason for the Note is that performing the Surveillance would perturb the electrical distribution system and challenge safety systems. This restriction from normally performing the Surveillance in MODE 1 or 2 is further amplified to allow portions of the Surveillance to be performed for the purpose of reestablishing OPERABILITY (e.g., post work testing following corrective maintenance, corrective modification, deficient or incomplete surveillance testing, and other unanticipated OPERABILITY concerns) provided an assessment determines plant safety is maintained or enhanced. This assessment shall, as a minimum, consider the potential outcomes and transients associated with a failed partial Surveillance, a successful partial Surveillance, and a perturbation of the offsite or onsite system when they are tied together or operated independently for the partial Surveillance; as well as the operator procedures available to cope with these outcomes. These shall be measured against the avoided risk of a plant shutdown and startup to determine that plant safety is maintained or enhanced when portions of the Surveillance are performed in MODE 1 or 2. Risk insights or deterministic methods may be used for the assessment. Credit may be taken for unplanned events that satisfy this SR.

BASES

REFERENCES

1. IEEE-450-[1995].
2. FSAR, Chapter [8].
3. FSAR, Chapter [6].
4. FSAR, Chapter [15].
5. IEEE-485-[1983], June 1983.

B 3.8 ELECTRICAL POWER SYSTEMS

B 3.8.7 Inverters - Operating

BASES

BACKGROUND

The inverters are the preferred source of power for the AC vital buses because of the stability and reliability they achieve. The function of the inverter is to provide AC electrical power to the vital buses. The inverters can be powered from an internal AC source/rectifier or from the station battery. The station battery provides an uninterruptible power source for the instrumentation and controls for the Reactor Protective System (RPS) and the Engineered Safety Feature Actuation System (ESFAS). Specific details on inverters and their operating characteristics are found in the FSAR, Chapter [8] (Ref. 1).

APPLICABLE SAFETY ANALYSES

The initial conditions of Design Basis Accident (DBA) and transient analyses in the FSAR, Chapter [6] (Ref. 2) and Chapter [15] (Ref. 3), assume Engineered Safety Feature systems are OPERABLE. The inverters are designed to provide the required capacity, capability, redundancy, and reliability to ensure the availability of necessary power to the RPS and ESFAS instrumentation and controls so that the fuel, Reactor Coolant System, and containment design limits are not exceeded. These limits are discussed in more detail in the Bases for Section 3.2, Power Distribution Limits; Section 3.4, Reactor Coolant System (RCS); and Section 3.6, Containment Systems.

The OPERABILITY of the inverters is consistent with the initial assumptions of the accident analyses and is based on meeting the design basis of the unit. This includes maintaining required AC vital buses OPERABLE during accident conditions in the event of:

a. An assumed loss of all offsite AC electrical power or all onsite AC electrical power and

b. A worst case single failure.

Inverters are a part of the distribution system and, as such, satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

The inverters ensure the availability of AC electrical power for the systems instrumentation required to shut down the reactor and maintain it in a safe condition after an anticipated operational occurrence (AOO) or a postulated DBA.

BASES

LCO (continued)

Maintaining the required inverters OPERABLE ensures that the redundancy incorporated into the design of the RPS and ESFAS instrumentation and controls is maintained. The four inverters [(two per train)] ensure an uninterruptible supply of AC electrical power to the AC vital buses even if the 4.16 kV safety buses are de-energized.

OPERABLE inverters require the associated vital bus to be powered by the inverter with output voltage and frequency within tolerances, and power input to the inverter from a [125 VDC] station battery. Alternatively, power supply may be from an internal AC source via rectifier as long as the station battery is available as the uninterruptible power supply.

This LCO is modified by a Note that allows [one/two] inverters to be disconnected from a [common] battery for ≤ 24 hours, if the vital bus(es) is powered from a [Class 1E constant voltage transformer or inverter using internal AC source] during the period and all other inverters are operable. This allows an equalizing charge to be placed on one battery. If the inverter(s) were not disconnected, the resulting voltage condition might damage the inverter(s). These provisions minimize the loss of equipment that would occur in the event of a loss of offsite power. The 24 hour time period for the allowance minimizes the time during which a loss of offsite power could result in the loss of equipment energized from the affected AC vital bus while taking into consideration the time required to perform an equalizing charge on the battery bank.

The intent of this Note is to limit the number of inverters that may be disconnected. Only those inverters associated with the single battery undergoing an equalizing charge may be disconnected. All other inverters must be aligned to their associated batteries, regardless of the number of inverters or unit design.

APPLICABILITY

The inverters are required to be OPERABLE in MODES 1, 2, 3, and 4 to ensure that:

a. Acceptable fuel design limits and reactor coolant pressure boundary limits are not exceeded as a result of AOOs or abnormal transients and

b. Adequate core cooling is provided, and containment OPERABILITY and other vital functions are maintained in the event of a postulated DBA.

Inverter requirements for MODES 5 and 6 are covered in the Bases for LCO 3.8.8, "Inverters - Shutdown."

BASES

ACTIONS

A.1

With a required inverter inoperable, its associated AC vital bus becomes inoperable until it is [manually] re-energized from its [Class 1E constant voltage source transformer or inverter using internal AC source].

Required Action A.1 is modified by a Note, which states to enter the applicable conditions and Required Actions of LCO 3.8.9, "Distribution Systems - Operating," when Condition A is entered with one AC vital bus de-energized. This ensures the vital bus is re-energized within 2 hours.

Required Action A.1 allows 24 hours to fix the inoperable inverter and return it to service. The 24 hour limit is based upon engineering judgment, taking into consideration the time required to repair an inverter and the additional risk to which the unit is exposed because of the inverter inoperability. This has to be balanced against the risk of an immediate shutdown, along with the potential challenges to safety systems such a shutdown might entail. When the AC vital bus is powered from its constant voltage source, it is relying upon interruptible AC electrical power sources (offsite and onsite). The uninterruptible inverter source to the AC vital buses is the preferred source for powering instrumentation trip setpoint devices.

B.1 and B.2

If the inoperable devices or components cannot be restored to OPERABLE status within the required Completion Time, the unit must be brought to a MODE in which the LCO does not apply. To achieve this status, the unit must be brought to at least MODE 3 within 6 hours and to MODE 5 within 36 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required unit conditions from full power conditions in an orderly manner and without challenging unit systems.

SURVEILLANCE REQUIREMENTS

SR 3.8.7.1

This Surveillance verifies that the inverters are functioning properly with all required circuit breakers closed and AC vital buses energized from the inverter. The verification of proper voltage and frequency output ensures that the required power is readily available for the instrumentation of the RPS and ESFAS connected to the AC vital buses. The 7 day Frequency takes into account the redundant capability of the inverters and other indications available in the control room that alert the operator to inverter malfunctions.

BASES

REFERENCES

1. FSAR, Chapter [8].

2. FSAR, Chapter [6].

3. FSAR, Chapter [14].

B 3.8 ELECTRICAL POWER SYSTEMS

B 3.8.8 Inverters - Shutdown

BASES

BACKGROUND	A description of the inverters is provided in the Bases for LCO 3.8.7, "Inverters - Operating."

APPLICABLE SAFETY ANALYSES

The initial conditions of Design Basis Accident (DBA) and transient analyses in the FSAR, Chapter [6] (Ref. 1) and Chapter [15] (Ref. 2), assume Engineered Safety Feature systems are OPERABLE. The DC to AC inverters are designed to provide the required capacity, capability, redundancy, and reliability to ensure the availability of necessary power to the Reactor Protective System and Engineered Safety Features Actuation System instrumentation and controls so that the fuel, Reactor Coolant System, and containment design limits are not exceeded.

The OPERABILITY of the inverters is consistent with the initial assumptions of the accident analyses and the requirements for the supported systems' OPERABILITY.

The OPERABILITY of the minimum inverters to each AC vital bus during MODES 5 and 6 ensures that:

a. The unit can be maintained in the shutdown or refueling condition for extended periods,

b. Sufficient instrumentation and control capability is available for monitoring and maintaining the unit status, and

c. Adequate power is available to mitigate events postulated during shutdown, such as a fuel handling accident [involving handling recently irradiated fuel. Due to radioactive decay, the inverters are only required to mitigate fuel handling accidents involving handling recently irradiated fuel (i.e., fuel that has occupied part of a critical reactor core within the previous [X] days)].

In general, when the unit is shut down, the Technical Specification requirements ensure that the unit has the capability to mitigate the consequences of postulated accidents. However, assuming a single failure and concurrent loss of all offsite or all onsite power is not required. The rationale for this is based on the fact that many DBAs that are analyzed in MODES [1, 2, 3, and 4] have no specific analyses in MODES [5 and 6] because the energy contained within the reactor

BASES

APPLICABLE SAFETY ANALYSES (continued)

pressure boundary, reactor coolant temperature and pressure, and the corresponding stresses result in the probabilities of occurrence being significantly reduced or eliminated, and in minimal consequences. These deviations from DBA analysis assumptions and design requirements during shutdown conditions are allowed by the LCO for required systems.

The shutdown Technical Specification requirements are designed to ensure that the unit has the capability to mitigate the consequences of certain postulated accidents. Worst case DBAs which are analyzed for operating MODES are generally viewed not to be a significant concern during shutdown MODES due to the lower energies involved. The Technical Specifications therefore require a lesser complement of electrical equipment to be available during shutdown than is required during operating MODES. More recent work completed on the potential risks associated with shutdown, however, have found significant risk associated with certain shutdown evolutions. As a result, in addition to the requirements established in the Technical Specifications, the industry has adopted NUMARC 91-06, "Guidelines for Industry Actions to Assess Shutdown Management," as an Industry initiative to manage shutdown tasks and associated electrical support to maintain risk at an acceptable low level. This may require the availability of additional equipment beyond that required by the shutdown Technical Specifications.

The inverters were previously identified as part of the distribution system and, as such, satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

The inverter[s] ensure the availability of electrical power for the instrumentation for systems required to shut down the reactor and maintain it in a safe condition after an anticipated operational occurrence or a postulated DBA. The battery powered inverter[s] provide[s] uninterruptible supply of AC electrical power to the AC vital bus[es] even if the 4.16 kV safety buses are de-energized. OPERABILITY of the inverter[s] requires that the vital bus be powered by the inverter. This ensures the availability of sufficient inverter power sources to operate the unit in a safe manner and to mitigate the consequences of postulated events during shutdown (e.g., fuel handling accidents [involving handling recently irradiated fuel]).

BASES

APPLICABILITY

The inverter[s] required to be OPERABLE in MODES 5 and 6 during movement of [recently] irradiated fuel assemblies provide assurance that:

a. Systems to provide adequate coolant inventory makeup are available for the irradiated fuel in the core,

b. Systems needed to mitigate a fuel handling accident [involving handling recently irradiated fuel (i.e., fuel that has occupied part of a critical reactor core within the previous [X] days)] are available,

c. Systems necessary to mitigate the effects of events that can lead to core damage during shutdown are available, and

d. Instrumentation and control capability is available for monitoring and maintaining the unit in a cold shutdown condition or refueling condition.

Inverter requirements for MODES 1, 2, 3, and 4 are covered in LCO 3.8.7.

ACTIONS

LCO 3.0.3 is not applicable while in MODE 5 or 6. However, since irradiated fuel assembly movement can occur in MODE 1, 2, 3, or 4, the ACTIONS have been modified by a Note stating that LCO 3.0.3 is not applicable. If moving irradiated fuel assemblies while in MODE 5 or 6, LCO .0.3 would not specify any action. If moving irradiated fuel assemblies while in MODE 1, 2, 3, or 4, the fuel movement is independent of reactor operations. Entering LCO 3.0.3, while in MODE 1, 2, 3, or 4 would require the unit to be shutdown unnecessarily.

A.1, A.2.1, A.2.2, A.2.3, and A.2.4

[If two trains are required by LCO 3.8.10, "Distribution Systems - Shutdown," the remaining OPERABLE inverters may be capable of supporting sufficient required features to allow continuation of CORE ALTERATIONS, [recently] irradiated fuel movement, operations with a potential for draining the reactor vessel, and operations with a potential for positive reactivity additions that could result in loss of required SDM (MODE 5) or boron concentration (MODE 6).] Suspending positive reactivity additions that could result in failure to meet the minimum SDM or boron concentration limit is required to assure continued safe

BASES

ACTIONS (continued)

operation. Introduction of coolant inventory must be from sources that have a boron concentration greater than that what would be required in the RCS for minimum SDM or refueling boron concentration. This may result in an overall reduction in RCS boron concentration, but provides acceptable margin to maintaining subcritical operation. Introduction of temperature changes including temperature increases when operating with a positive MTC must also be evaluated to ensure they do not result in a loss of required SDM. By the allowance of the option to declare required features inoperable with the associated inverter(s) inoperable, appropriate restrictions will be implemented in accordance with the affected required features LCOs' Required Actions. In many instances, this option may involve undesired administrative efforts. Therefore, the allowance for sufficiently conservative actions is made (i.e., to suspend CORE ALTERATIONS, movement of [recently] irradiated fuel assemblies, and operations involving positive reactivity additions).

Suspension of these activities shall not preclude completion of actions to establish a safe conservative condition. These actions minimize the probability of the occurrence of postulated events. It is further required to immediately initiate action to restore the required inverter[s] and to continue this action until restoration is accomplished in order to provide the necessary inverter power to the unit safety systems.

The Completion Time of immediately is consistent with the required times for actions requiring prompt attention. The restoration of the required inverters should be completed as quickly as possible in order to minimize the time the unit safety systems may be without power or powered from a constant voltage source transformer.

SURVEILLANCE REQUIREMENTS

SR 3.8.8.1

This Surveillance verifies that the inverters are functioning properly with all required circuit breakers closed and AC vital buses energized from the inverter. The verification of proper voltage and frequency output ensures that the required power is readily available for the instrumentation connected to the AC vital buses. The 7 day Frequency takes into account the redundant capability of the inverters and other indications available in the control room that alert the operator to inverter malfunctions.

REFERENCES

1. FSAR, Chapter [6].

2. FSAR, Chapter [15].

B 3.8 ELECTRICAL POWER SYSTEMS

B 3.8.9 Distribution Systems - Operating

BASES

BACKGROUND

The onsite Class 1E AC, DC, and AC vital bus electrical power distribution systems are divided by train into [two] redundant and independent AC, DC, and AC vital bus electrical power distribution subsystems.

The AC electrical power subsystem for each train consists of a 4.16 kV Engineered Safety Feature (ESF) bus, having at least [one separate and independent offsite source of power] as well as a dedicated onsite diesel generator (DG) source. Each [4.16 kV ESF bus] is normally connected to a preferred offsite source. After a loss of the preferred offsite power source to a 4.16 kV ESF bus, a transfer to the alternate offsite source is accomplished by utilizing a time delayed bus undervoltage relay. If all offsite sources are unavailable, the onsite emergency DG supplies power to the 4.16 kV ESF bus. Control power for the 4.16 kV breakers is supplied from the Class 1E batteries. Additional description of this system may be found in the Bases for LCO 3.8.1, "AC Sources - Operating," and the Bases for LCO 3.8.4, "DC Sources - Operating."

The secondary AC electrical power distribution subsystem for each train includes the safety related load centers, motor control centers, and distribution panels shown in Table B 3.8.9-1.

The 120 VAC vital buses are arranged in two load groups per train and are normally powered from the inverters. The alternate power supply for the vital buses are Class 1E constant voltage source transformers powered from the same train as the associated inverter, and its use is governed by LCO 3.8.7, "Inverters - Operating." Each constant voltage source transformer is powered from a Class 1E AC bus.

The DC electrical power distribution subsystem consists of [125] V bus(es) and distribution panel(s).

The list of all required DC and vital AC distribution buses [and panels] is presented in Table B 3.8.9-1.

BASES

APPLICABLE SAFETY ANALYSES

The initial conditions of Design Basis Accident (DBA) and transient analyses in the FSAR, Chapter [6] (Ref. 1) and Chapter [15] (Ref. 2), assume ESF systems are OPERABLE. The AC, DC, and AC vital bus electrical power distribution systems are designed to provide sufficient capacity, capability, redundancy, and reliability to ensure the availability of necessary power to ESF systems so that the fuel, Reactor Coolant System, and containment design limits are not exceeded. These limits are discussed in more detail in the Bases for Section 3.2, Power Distribution Limits; Section 3.4, Reactor Coolant System (RCS); and Section 3.6, Containment Systems.

The OPERABILITY of the AC, DC, and AC vital bus electrical power distribution systems is consistent with the initial assumptions of the accident analyses and is based upon meeting the design basis of the unit. This includes maintaining power distribution systems OPERABLE during accident conditions in the event of:

a. An assumed loss of all offsite power or all onsite AC electrical power and

b. A worst case single failure.

The distribution systems satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

The required power distribution subsystems listed in Table B 3.8.9-1 ensure the availability of AC, DC, and AC vital bus electrical power for the systems required to shut down the reactor and maintain it in a safe condition after an anticipated operational occurrence (AOO) or a postulated DBA. The AC, DC, and AC vital bus electrical power distribution subsystems are required to be OPERABLE.

Maintaining the Train A and Train B AC, DC, and AC vital bus electrical power distribution subsystems OPERABLE ensures that the redundancy incorporated into the design of ESF is not defeated. Therefore, a single failure within any system or within the electrical power distribution subsystems will not prevent safe shutdown of the reactor.

OPERABLE AC electrical power distribution subsystems require the associated buses, load centers, motor control centers, and distribution panels to be energized to their proper voltages. OPERABLE DC electrical power distribution subsystems require the associated buses and distribution panels to be energized to their proper voltage from either the associated battery or charger. OPERABLE vital bus electrical power distribution subsystems require the associated buses to be energized to their proper voltage from the associated [inverter via inverted DC voltage, inverter using internal AC source, or Class 1E constant voltage transformer].

BASES

LCO (continued)

In addition, tie breakers between redundant safety related AC, DC, and AC vital bus power distribution subsystems, if they exist, must be open. This prevents any electrical malfunction in any power distribution subsystem from propagating to the redundant subsystem, which could cause the failure of a redundant subsystem and a loss of essential safety function(s). If any tie breakers are closed, the affected redundant electrical power distribution subsystems are considered inoperable. This applies to the onsite, safety related redundant electrical power distribution subsystems. It does not, however, preclude redundant Class 1E 4.16 kV buses from being powered from the same offsite circuit.

APPLICABILITY

The electrical power distribution subsystems are required to be OPERABLE in MODES 1, 2, 3, and 4 to ensure that:

a. Acceptable fuel design limits and reactor coolant pressure boundary limits are not exceeded as a result of AOOs or abnormal transients and

b. Adequate core cooling is provided, and containment OPERABILITY and other vital functions are maintained in the event of a postulated DBA.

Electrical power distribution subsystem requirements for MODES 5 and 6 are covered in the Bases for LCO 3.8.10, "Distribution Systems - Shutdown."

ACTIONS

A.1

With one or more Train A and B required AC buses, load centers, motor control centers, or distribution panels (except AC vital buses), in one train inoperable and a loss of function has not occurred, the remaining AC electrical power distribution subsystems are capable of supporting the minimum safety functions necessary to shut down the reactor and maintain it in a safe shutdown condition, assuming no single failure. The overall reliability is reduced, however, because a single failure in the remaining power distribution subsystems could result in the minimum required ESF functions not being supported. Therefore, the required AC buses, load centers, motor control centers, and distribution panels must be restored to OPERABLE status within 8 hours.

BASES

ACTIONS (continued)

Condition A worst scenario is one train without AC power (i.e., no offsite power to the train and the associated DG inoperable). In this condition, the unit is more vulnerable to a complete loss of AC power. It is, therefore, imperative that the unit operator's attention be focused on minimizing the potential for loss of power to the remaining train by stabilizing the unit, and on restoring power to the affected train. The 8 hour time limit before requiring a unit shutdown in this condition is acceptable because of:

a. The potential for decreased safety if the unit operator's attention is diverted from the evaluations and actions necessary to restore power to the affected train, to the actions associated with taking the unit to shutdown within this time limit and

b. The potential for an event in conjunction with a single failure of a redundant component in the train with AC power.

Required Action A.1 is modified by a Note that requires the applicable Conditions and Required Actions of LCO 3.8.4, "DC Sources - Operating," to be entered for DC trains made inoperable by inoperable power distribution subsystems. This is an exception to LCO 3.0.6 and ensures the proper actions are taken for these components. Inoperability of a distribution system can result in loss of charging power to batteries and eventual loss of DC power. This Note ensures that the appropriate attention is given to restoring charging power to batteries, if necessary, after loss of distribution systems.

B.1

With one or more AC vital buses inoperable, and a loss of function has not yet occurred, the remaining OPERABLE AC vital buses are capable of supporting the minimum safety functions necessary to shut down the unit and maintain it in the safe shutdown condition. Overall reliability is reduced, however, since an additional single failure could result in the minimum required ESF functions not being supported. Therefore, the [required] AC vital bus must be restored to OPERABLE status within 2 hours by powering the bus from the associated [inverter via inverted DC, inverter using internal AC source, or Class 1E constant voltage transformer].

BASES

ACTIONS (continued)

Condition B represents one or more AC vital buses without power; potentially both the DC source and the associated AC source are nonfunctioning. In this situation, the unit is significantly more vulnerable to a complete loss of all noninterruptible power. It is, therefore, imperative that the operator's attention focus on stabilizing the unit, minimizing the potential for loss of power to the remaining vital buses, and restoring power to the affected vital bus.

This 2 hour limit is more conservative than Completion Times allowed for the vast majority of components that are without adequate vital AC power. Taking exception to LCO 3.0.2 for components without adequate vital AC power, which would have the Required Action Completion Times shorter than 2 hours if declared inoperable, is acceptable because of:

a. The potential for decreased safety by requiring a change in unit conditions (i.e., requiring a shutdown) and not allowing stable operations to continue,

b. The potential for decreased safety by requiring entry into numerous Applicable Conditions and Required Actions for components without adequate vital AC power and not providing sufficient time for the operators to perform the necessary evaluations and actions for restoring power to the affected train, and

c. The potential for an event in conjunction with a single failure of a redundant component.

The 2 hour Completion Time takes into account the importance to safety of restoring the AC vital bus to OPERABLE status, the redundant capability afforded by the other OPERABLE vital buses, and the low probability of a DBA occurring during this period.

<u>C.1</u>

With one or more DC buses or distribution panels inoperable, and a loss of function has not yet occurred, the remaining DC electrical power distribution subsystems are capable of supporting the minimum safety functions necessary to shut down the reactor and maintain it in a safe shutdown condition, assuming no single failure. The overall reliability is reduced, however, because a single failure in the remaining DC electrical power distribution subsystem could result in the minimum required ESF functions not being supported. Therefore, the [required] DC buses and distribution panels must be restored to OPERABLE status within 2 hours by powering the bus from the associated battery or charger.

BASES

ACTIONS (continued)

Condition C represents one or more DC buses or distribution panels without adequate DC power; potentially both with the battery significantly degraded and the associated charger nonfunctioning. In this situation, the unit is significantly more vulnerable to a complete loss of all DC power. It is, therefore, imperative that the operator's attention focus on stabilizing the unit, minimizing the potential for loss of power to the remaining trains and restoring power to the affected train.

This 2 hour limit is more conservative than Completion Times allowed for the vast majority of components which would be without power. Taking exception to LCO 3.0.2 for components without adequate DC power, which would have Required Action Completion Times shorter than 2 hours, is acceptable because of:

a. The potential for decreased safety by requiring a change in unit conditions (i.e., requiring a shutdown) while allowing stable operations to continue,

b. The potential for decreased safety by requiring entry into numerous applicable Conditions and Required Actions for components without DC power and not providing sufficient time for the operators to perform the necessary evaluations and actions for restoring power to the affected train, and

c. The potential for an event in conjunction with a single failure of a redundant component.

The 2 hour Completion Time for DC buses is consistent with Regulatory Guide 1.93 (Ref. 3).

D.1 and D.2

If the inoperable distribution subsystem cannot be restored to OPERABLE status within the required Completion Time, the unit must be brought to a MODE in which the LCO does not apply. To achieve this status, the unit must be brought to at least MODE 3 within 6 hours and to MODE 5 within 36 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required unit conditions from full power conditions in an orderly manner and without challenging unit systems.

BASES

ACTIONS (continued)

E.1

Condition E corresponds to a level of degradation in the electrical distribution system that causes a required safety function to be lost. When more than one inoperable electrical power distribution subsystem results in the loss of a required function, the plant is in a condition outside the accident analysis. Therefore, no additional time is justified for continued operation. LCO 3.0.3 must be entered immediately to commence a controlled shutdown.

SURVEILLANCE REQUIREMENTS

SR 3.8.9.1

This Surveillance verifies that the AC, DC, and AC vital bus electrical power distribution systems are functioning properly, with the correct circuit breaker alignment. The correct breaker alignment ensures the appropriate separation and independence of the electrical divisions is maintained, and the appropriate voltage is available to each required bus. The verification of proper voltage availability on the buses ensures that the required voltage is readily available for motive as well as control functions for critical system loads connected to these buses. The 7 day Frequency takes into account the redundant capability of the AC, DC, and AC vital bus electrical power distribution subsystems, and other indications available in the control room that alert the operator to subsystem malfunctions.

REFERENCES

1. FSAR, Chapter [6].

2. FSAR, Chapter [15].

3. Regulatory Guide 1.93, December 1974.

Table B 3.8.9-1 (page 1 of 1)
AC and DC Electrical Power Distribution Systems

TYPE	VOLTAGE	TRAIN A*	TRAIN B*
AC safety buses	[4160 V]	[ESF Bus] [NB01]	[ESF Bus] [NB02]
	[480 V]	Load Centers [NG01, NG03]	Load Centers [NG02, NG04]
	[480 V]	Motor Control Centers [NG01A, NG01I, NG01B, NG03C, NG03I, NG03D]	Motor Control Centers [NG02A, NG02I, NG02B, NG04C, NG04I, NG04D]
	[120 V]	Distribution Panels [NP01, NP03]	Distribution Panels [NP02, NP04]
DC buses	[125 V]	Bus [NK01]	Bus [NK02]
		Bus [NK03]	Bus [NK04]
		Distribution Panels [NK41, NK43, NK51]	Distribution Panels [NK42, NK44, NK52]
AC vital buses	[120 V]	Bus [NN01]	Bus [NN02]
		Bus [NN03]	Bus [NN04]

* Each train of the AC and DC electrical power distribution systems is a subsystem.

B 3.8 ELECTRICAL POWER SYSTEMS

B 3.8.10 Distribution Systems - Shutdown

BASES

BACKGROUND	A description of the AC, DC, and AC vital bus electrical power distribution systems is provided in the Bases for LCO 3.8.9, "Distribution Systems - Operating."

APPLICABLE SAFETY ANALYSES

The initial conditions of Design Basis Accident and transient analyses in the FSAR, Chapter [6] (Ref. 1) and Chapter [15] (Ref. 2), assume Engineered Safety Feature (ESF) systems are OPERABLE. The AC, DC, and AC vital bus electrical power distribution systems are designed to provide sufficient capacity, capability, redundancy, and reliability to ensure the availability of necessary power to ESF systems so that the fuel, Reactor Coolant System, and containment design limits are not exceeded.

The OPERABILITY of the AC, DC, and AC vital bus electrical power distribution system is consistent with the initial assumptions of the accident analyses and the requirements for the supported systems' OPERABILITY.

The OPERABILITY of the minimum AC, DC, and AC vital bus electrical power distribution subsystems during MODES 5 and 6, and during movement of [recently] irradiated fuel assemblies, ensures that:

a. The unit can be maintained in the shutdown or refueling condition for extended periods,

b. Sufficient instrumentation and control capability is available for monitoring and maintaining the unit status, and

c. Adequate power is provided to mitigate events postulated during shutdown, such as a fuel handling accident [involving handling recently irradiated fuel. Due to radioactive decay, AC, DC, and AC vital bus electrical power is only required to mitigate fuel handling accidents involving handling recently irradiated fuel (i.e., fuel that has occupied part of a critical reactor core within the previous [X] days)].

The AC and DC electrical power distribution systems satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO

Various combinations of subsystems, equipment, and components are required OPERABLE by other LCOs, depending on the specific unit condition. Implicit in those requirements is the required OPERABILITY of necessary support required features. This LCO explicitly requires energization of the portions of the electrical distribution system necessary to support OPERABILITY of required systems, equipment and components - all specifically addressed in each LCO and implicitly required via the definition of OPERABILITY.

Maintaining these portions of the distribution system energized ensures the availability of sufficient power to operate the unit in a safe manner to mitigate the consequences of postulated events during shutdown (e.g., fuel handling accidents [involving handling recently irradiated fuel]).

APPLICABILITY

The AC and DC electrical power distribution subsystems required to be OPERABLE in MODES 5 and 6, and during movement of [recently] irradiated fuel assemblies, provide assurance that:

a. Systems to provide adequate coolant inventory makeup are available for the irradiated fuel in the core,

b. Systems needed to mitigate a fuel handling accident [involving handling recently irradiated fuel (i.e., fuel that has occupied part of a critical reactor core within the previous [X] days)] are available,

c. Systems necessary to mitigate the effects of events that can lead to core damage during shutdown are available, and

d. Instrumentation and control capability is available for monitoring and maintaining the unit in a cold shutdown condition and refueling condition.

The AC, DC, and AC vital bus electrical power distribution subsystem requirements for MODES 1, 2, 3, and 4 are covered in LCO 3.8.9.

ACTIONS

LCO 3.0.3 is not applicable while in MODE 5 or 6. However, since irradiated fuel assembly movement can occur in MODE 1, 2, 3, or 4, the ACTIONS have been modified by a Note stating that LCO 3.0.3 is not applicable. If moving irradiated fuel assemblies while in MODE 5 or 6, LCO 3.0.3 would not specify any action. If moving irradiated fuel assemblies while in MODE 1, 2, 3, or 4, the fuel movement is independent of reactor operations. Entering LCO 3.0.3, while in MODE 1, 2, 3, or 4 would require the unit to be shutdown unnecessarily.

BASES

ACTIONS (continued)

A.1, A.2.1, A.2.2, A.2.3, A.2.4, and A.2.5

Although redundant required features may require redundant trains of electrical power distribution subsystems to be OPERABLE, one OPERABLE distribution subsystem train may be capable of supporting sufficient required features to allow continuation of CORE ALTERATIONS and [recently] irradiated fuel movement. By allowing the option to declare required features associated with an inoperable distribution subsystem inoperable, appropriate restrictions are implemented in accordance with the affected distribution subsystems LCO's Required Actions. In many instances, this option may involve undesired administrative efforts. Therefore, the allowance for sufficiently conservative actions is made (i.e., to suspend CORE ALTERATIONS, movement of [recently] irradiated fuel assemblies, and operations involving positive reactivity additions that could result in loss of required SDM (MODE 5) or boron concentration (MODE 6). Suspending positive reactivity additions that could result in failure to meet the minimum SDM or boron concentration limit is required to assure continued safe operation. Introduction of coolant inventory must be from sources that have a boron concentration greater than that what would be required in the RCS for minimum SDM or refueling boron concentration. This may result in an overall reduction in RCS boron concentration, but provides acceptable margin to maintaining subcritical operation. Introduction of temperature changes including temperature increases when operating with a positive MTC must also be evaluated to ensure they do not result in a loss of required SDM.

Suspension of these activities shall not preclude completion of actions to establish a safe conservative condition. These actions minimize the probability of the occurrence of postulated events. It is further required to immediately initiate action to restore the required AC and DC electrical power distribution subsystems and to continue this action until restoration is accomplished in order to provide the necessary power to the unit safety systems.

Notwithstanding performance of the above conservative Required Actions, a required shutdown cooling (SDC) subsystem may be inoperable. In this case, Required Actions A.2.1 through A.2.4 do not adequately address the concerns relating to coolant circulation and heat removal. Pursuant to LCO 3.0.6, the SDC ACTIONS would not be entered. Therefore, Required Action A.2.5 is provided to direct declaring SDC inoperable, which results in taking the appropriate SDC actions.

BASES

ACTIONS (continued)

The Completion Time of immediately is consistent with the required times for actions requiring prompt attention. The restoration of the required distribution subsystems should be completed as quickly as possible in order to minimize the time the unit safety systems may be without power.

SURVEILLANCE REQUIREMENTS

SR 3.8.10.1

This Surveillance verifies that the AC, DC, and AC vital bus electrical power distribution system is functioning properly, with all the buses energized. The verification of proper voltage availability on the buses ensures that the required power is readily available for motive as well as control functions for critical system loads connected to these buses. The 7 day Frequency takes into account the redundant capability of the electrical power distribution subsystems, and other indications available in the control room that alert the operator to subsystem malfunctions.

REFERENCES

1. FSAR, Chapter [6].

2. FSAR, Chapter [15].

B 3.9 REFUELING OPERATIONS

B 3.9.1 Boron Concentration

BASES

BACKGROUND

The limit on the boron concentrations of the Reactor Coolant System (RCS), the refueling canal, and refueling cavity during refueling ensures that the reactor remains subcritical during MODE 6. Refueling boron concentration is the soluble boron concentration in the coolant in each of these volumes having direct access to the reactor core during refueling.

The soluble boron concentration offsets the core reactivity and is measured by chemical analysis of a representative sample of the coolant in each of the volumes. The refueling boron concentration limit is specified in the COLR. Unit procedures ensure the specified boron concentration in order to maintain an overall core reactivity of $k_{eff} \leq 0.95$ during fuel handling, with control element assemblies (CEAs) and fuel assemblies assumed to be in the most adverse configuration (least negative reactivity) allowed by unit procedures.

GDC 26 of 10 CFR 50, Appendix A, requires that two independent reactivity control systems of different design principles be provided (Ref. 1). One of these systems must be capable of holding the reactor core subcritical under cold conditions. The Chemical and Volume Control System (CVCS) is the system capable of maintaining the reactor subcritical in cold conditions by maintaining the boron concentration.

The reactor is brought to shutdown conditions before beginning operations to open the reactor vessel for refueling. After the RCS is cooled and depressurized and the vessel head is unbolted, the head is slowly removed to form the refueling cavity. The refueling canal and the refueling cavity are then flooded with borated water from the refueling water tank into the open reactor vessel by gravity feeding or by the use of the Shutdown Cooling (SDC) System pumps.

The pumping action of the SDC System in the RCS and the natural circulation due to thermal driving heads in the reactor vessel and the refueling cavity mix the added concentrated boric acid with the water in the refueling canal. The SDC System is in operation during refueling (see LCO 3.9.4, "Shutdown Cooling and Coolant Circulation - High Water Level," and LCO 3.9.5, "Shutdown Cooling and Coolant Circulation - Low Water Level") to provide forced circulation in the RCS and assist in maintaining the boron concentrations in the RCS, the refueling canal, and the refueling cavity above the COLR limit.

BASES

APPLICABLE SAFETY ANALYSES

During refueling operations, the reactivity condition of the core is consistent with the initial conditions assumed for the boron dilution accident in the accident analysis and is conservative for MODE 6. The boron concentration limit specified in the COLR is based on the core reactivity at the beginning of each fuel cycle (the end of refueling) and includes an uncertainty allowance.

The required boron concentration and the unit refueling procedures that demonstrate the correct fuel loading plan (including full core mapping) ensure the k_{eff} of the core will remain ≤ 0.95 during the refueling operation. Hence, at least a 5% $\Delta k/k$ margin of safety is established during refueling.

During refueling, the water volume in the spent fuel pool, the transfer canal, the refueling canal, the refueling cavity, and the reactor vessel form a single mass. As a result, the soluble boron concentration is relatively the same in each of these volumes.

The limiting boron dilution accident analyzed occurs in MODE 5 (Ref. 2). A detailed discussion of this event is provided in B 3.1.1, “SHUTDOWN MARGIN (SDM).”

The RCS boron concentration satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

The LCO requires that a minimum boron concentration be maintained in the RCS, the refueling canal, and refueling cavity while in MODE 6. The boron concentration limit specified in the COLR ensures a core k_{eff} of ≤ 0.95 is maintained during fuel handling operations. Violation of the LCO could lead to an inadvertent criticality during MODE 6.

APPLICABILITY

This LCO is applicable in MODE 6 to ensure that the fuel in the reactor vessel will remain subcritical. The required boron concentration ensures a $k_{eff} \leq 0.95$. Above MODE 6, LCO 3.1.1, "SHUTDOWN MARGIN (SDM)," ensures that an adequate amount of negative reactivity is available to shut down the reactor and to maintain it subcritical.

The Applicability is modified by a Note. The Note states that the limits on boron concentration are only applicable to the refueling canal and the refueling cavity when those volumes are connected to the RCS. When the refueling canal and the refueling cavity are isolated from the RCS, no potential path for boron dilution exists.

BASES

ACTIONS

A.1 and A.2

Continuation of CORE ALTERATIONS or positive reactivity additions (including actions to reduce boron concentration) is contingent upon maintaining the unit in compliance with the LCO. If the boron concentration of any coolant volume in the RCS, the refueling canal, or the refueling cavity is less than its limit, all operations involving CORE ALTERATIONS or positive reactivity additions must be suspended immediately. Operations that individually add limited positive reactivity (e.g., temperature fluctuations from inventory addition or temperature control fluctuations), but when combined with all other operations affecting core reactivity (e.g., intentional boration) result in overall net negative reactivity addition, are not precluded by this action.

Suspension of CORE ALTERATIONS and positive reactivity additions shall not preclude moving a component to a safe position.

A.3

In addition to immediately suspending CORE ALTERATIONS and positive reactivity additions, boration to restore the concentration must be initiated immediately.

In determining the required combination of boration flow rate and concentration, there is no unique design basis event that must be satisfied. The only requirement is to restore the boron concentration to its required value as soon as possible. In order to raise the boron concentration as soon as possible, the operator should begin boration with the best source available for unit conditions.

Once boration is initiated, it must be continued until the boron concentration is restored. The restoration time depends on the amount of boron that must be injected to reach the required concentration.

SURVEILLANCE REQUIREMENTS

SR 3.9.1.1

This SR ensures the coolant boron concentration in the RCS, and connected portions of the refueling canal and the refueling cavity, is within the COLR limits. The boron concentration of the coolant in each required volume is determined periodically by chemical analysis. Prior to re-connecting portions of the refueling canal or the refueling cavity to the RCS, this SR must be met per SR 3.0.4. If any dilution activity has occurred while the cavity or canal were disconnected from the RCS, this SR ensures the correct boron concentration prior to communication with the RCS.

BASES

SURVEILLANCE REQUIREMENTS (continued)

A minimum Frequency of once every 72 hours is therefore a reasonable amount of time to verify the boron concentration of representative samples. The Frequency is based on operating experience, which has shown 72 hours to be adequate.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 26.

2. FSAR, Section [ ].

B 3.9 REFUELING OPERATIONS

B 3.9.2 Nuclear Instrumentation

BASES

BACKGROUND	The source range monitors (SRMs) are used during refueling operations to monitor the core reactivity condition. The installed SRMs are part of the Nuclear Instrumentation System (NIS). These detectors are located external to the reactor vessel and detect neutrons leaking from the core. The use of portable detectors is permitted, provided the LCO requirements are met. The installed SRMs are BF3 detectors operating in the proportional region of the gas filled detector characteristic curve. The detectors monitor the neutron flux in counts per second. The instrument range covers five decades of neutron flux (1E+5 cps) with a [5%] instrument accuracy. The detectors also provide continuous visual indication in the control room and an audible alarm to alert operators to a possible dilution accident. The NIS is designed in accordance with the criteria presented in Reference 1. If used, portable detectors should be functionally equivalent to the NIS SRMs.
APPLICABLE SAFETY ANALYSES	Two OPERABLE SRMs are required to provide a signal to alert the operator to unexpected changes in core reactivity such as by a boron dilution accident or an improperly loaded fuel assembly. The safety analysis of the uncontrolled boron dilution accident is described in Reference 2. The analysis of the uncontrolled boron dilution accident shows that normally available SHUTDOWN MARGIN would be reduced, but there is sufficient time for the operator to take corrective actions. The SRMs satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).
LCO	This LCO requires two SRMs OPERABLE to ensure that redundant monitoring capability is available to detect changes in core reactivity.
APPLICABILITY	In MODE 6, the SRMs must be OPERABLE to determine changes in core reactivity. There is no other direct means available to check core reactivity levels. In MODES 2, 3, 4, and 5, the installed source range detectors and circuitry are required to be OPERABLE by LCO 3.3.2, "RPS Instrumentation Shutdown."

BASES

ACTIONS

A.1 and A.2

With only one SRM OPERABLE, redundancy has been lost. Since these instruments are the only direct means of monitoring core reactivity conditions, CORE ALTERATIONS and introduction of coolant into the RCS with boron concentration less than required to meet the minimum boron concentration of LCO 3.9.1 must be suspended immediately. Suspending positive reactivity additions that could result in failure to meet the minimum boron concentration limit is required to assure continued safe operation. Introduction of coolant inventory must be from sources that have a boron concentration greater than that what would be required in the RCS for minimum refueling boron concentration. This may result in an overall reduction in RCS boron concentration, but provides acceptable margin to maintaining subcritical operation. Performance of Required Action A.1 shall not preclude completion of movement of a component to a safe position.

B.1

With no SRM OPERABLE, action to restore a monitor to OPERABLE status shall be initiated immediately. Once initiated, action shall be continued until an SRM is restored to OPERABLE status.

B.2

With no SRM OPERABLE, there is no direct means of detecting changes in core reactivity. However, since CORE ALTERATIONS and positive reactivity additions are not to be made, the core reactivity condition is stabilized until the SRMs are OPERABLE. This stabilized condition is determined by performing SR 3.9.1.1 to verify that the required boron concentration exists.

The Completion Time of once per 12 hours is sufficient to obtain and analyze a reactor coolant sample for boron concentration and ensures that unplanned changes in boron concentration would be identified. The 12 hour Frequency is reasonable, considering the low probability of a change in core reactivity during this period.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.9.2.1

SR 3.9.2.1 is the performance of a CHANNEL CHECK, which is a comparison of the parameter indicated on one channel to a similar parameter on other channels. It is based on the assumption that the two indication channels should be consistent with core conditions. Changes in fuel loading and core geometry can result in significant differences between source range channels, but each channel should be consistent with its local conditions.

The Frequency of 12 hours is consistent with the CHANNEL CHECK Frequency specified similarly for the same instruments in LCO 3.3.1, "Reactor Protection System."

SR 3.9.2.2

SR 3.9.2.2 is the performance of a CHANNEL CALIBRATION every 18 months. This SR is modified by a Note stating that neutron detectors are excluded from the CHANNEL CALIBRATION. The CHANNEL CALIBRATION for the source range neutron flux monitors consists of obtaining the detector plateau or preamp discriminator curves, evaluating those curves, and comparing the curves to the manufacturer's data. The 18 month Frequency is based on the need to perform this Surveillance under the conditions that apply during a plant outage. Operating experience has shown these components usually pass the Surveillance when performed on the 18 month Frequency.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 13, GDC 26, GDC 28, and GDC 29.

2. FSAR, Section [ ].

B 3.9 REFUELING OPERATIONS

B 3.9.3 Containment Penetrations

BASES

BACKGROUND

During movement of [recently] irradiated fuel assemblies within containment, a release of fission product radioactivity within the containment will be restricted from escaping to the environment when the LCO requirements are met. In MODES 1, 2, 3, and 4, this is accomplished by maintaining containment OPERABLE as described in LCO 3.6.1, "Containment." In MODE 6, the potential for containment pressurization as a result of an accident is not likely; therefore, requirements to isolate the containment from the outside atmosphere can be less stringent. The LCO requirements are referred to as "containment closure" rather than "containment OPERABILITY." Containment closure means that all potential escape paths are closed or capable of being closed. Since there is no potential for containment pressurization, the Appendix J leakage criteria and tests are not required.

The containment serves to contain fission product radioactivity that may be released from the reactor core following an accident, such that offsite radiation exposures are maintained well within the requirements of 10 CFR 100. Additionally, the containment structure provides radiation shielding from the fission products that may be present in the containment atmosphere following accident conditions.

The containment equipment hatch, which is part of the containment pressure boundary, provides a means for moving large equipment and components into and out of containment. During movement of [recently] irradiated fuel assemblies within containment, the equipment hatch must be held in place by at least four bolts. Good engineering practice dictates that the bolts required by this LCO be approximately equally spaced.

The containment air locks, which are also part of the containment pressure boundary, provide a means for personnel access during MODES 1, 2, 3, and 4 operation in accordance with LCO 3.6.2, "Containment Air Locks." Each air lock has a door at both ends. The doors are normally interlocked to prevent simultaneous opening when containment OPERABILITY is required. During periods of shutdown when containment closure is not required, the door interlock mechanism may be disabled, allowing both doors of an air lock to remain open for extended periods when frequent containment entry is necessary. During movement of [recently] irradiated fuel assemblies within containment, containment closure is required; therefore, the door interlock mechanism may remain disabled, but one air lock door must always remain [capable of being] closed.

BASES

BACKGROUND (continued)

The requirements on containment penetration closure ensure that a release of fission product radioactivity within containment will be restricted to within regulatory limits.

The Containment Purge and Exhaust System includes two subsystems. The normal subsystem includes a 42 inch purge penetration and a 42 inch exhaust penetration. The second subsystem, a minipurge system, includes an 8 inch purge penetration and an 8 inch exhaust penetration. During MODES 1, 2, 3, and 4, the two valves in each of the normal purge and exhaust penetrations are secured in the closed position. The two valves in each of the two minipurge penetrations can be opened intermittently, but are closed automatically by the Engineered Safety Features Actuation System (ESFAS). Neither of the subsystems is subject to a Specification in MODE 5.

In MODE 6, large air exchanges are necessary to conduct refueling operations. The normal 42 inch purge system is used for this purpose and all valves are closed by the ESFAS in accordance with LCO 3.3.2, "Reactor Protective System (RPS) - Shutdown."

[The minipurge system remains operational in MODE 6 and all four valves are also closed by the ESFAS.

[or]

The minipurge system is not used in MODE 6. All four [8] inch valves are secured in the closed position.]

The other containment penetrations that provide direct access from containment atmosphere to outside atmosphere must be isolated on at least one side. Isolation may be achieved by an OPERABLE automatic isolation valve, or by a manual isolation valve, blind flange, or equivalent. Equivalent isolation methods must be approved and may include use of a material that can provide a temporary, atmospheric pressure ventilation barrier for the other containment penetrations during [recently] irradiated fuel movements (Ref. 1).

APPLICABLE SAFETY ANALYSES

During CORE ALTERATIONS or movement of irradiated fuel assemblies within containment, the most severe radiological consequences result from a fuel handling accident [involving handling recently irradiated fuel]. The fuel handling accident is a postulated event that involves damage to irradiated fuel (Ref. 2). Fuel handling accidents, analyzed in Ref. 3,

BASES

APPLICABLE SAFETY ANALYSES (continued)

include dropping a single irradiated fuel assembly and handling tool or a heavy object onto other irradiated fuel assemblies. The requirements of LCO 3.9.6, "Refueling Water Level," in conjunction with minimum decay time of [72] hours prior to [irradiated fuel movement with containment closure capability or a minimum decay time of [x] days without containment closure capability], ensure that the release of fission product radioactivity, subsequent to a fuel handling accident, results in doses that are well within the guideline values specified in 10 CFR 100. The acceptance limits for offsite radiation exposure are contained in Standard Review Plan Section 15.7.4, Rev. 1 (Ref. 3), which defines "well within" 10 CFR 100 to be 25% or less of the 10 CFR 100 values.

Containment penetrations satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

-----------------------------------REVIEWER'S NOTE-----------------------------------
The allowance to have containment personnel air lock doors open and penetration flow paths with direct access from the containment atmosphere to the outside atmosphere to be unisolated during fuel movement and CORE ALTERATIONS is based on (1) confirmatory dose calculations of a fuel handling accident as approved by the NRC staff which indicate acceptable radiological consequences and (2) commitments from the licensee to implement acceptable administrative procedures that ensure in the event of a refueling accident (even though the containment fission product control function is not required to meet acceptable dose consequences) that the open air lock can and will be promptly closed following containment evacuation and that the open penetration(s) can and will be promptly closed. The time to close penetrations or combination of penetrations shall be included in the confirmatory dose calculations.

This LCO limits the consequences of a fuel handling accident [involving handling recently irradiated fuel] in containment by limiting the potential escape paths for fission product radioactivity released within containment. The LCO requires any penetration providing direct access from the containment atmosphere to the outside atmosphere to be closed except for the OPERABLE containment purge and exhaust penetrations [and the containment personnel air locks]. For the OPERABLE containment purge and exhaust penetrations, this LCO ensures that these penetrations are isolable by the Containment Purge and Exhaust Isolation System. The

BASES

LCO (continued)

OPERABILITY requirements for this LCO ensure that the automatic purge and exhaust valve closure times specified in the FSAR can be achieved and therefore meet the assumptions used in the safety analysis to ensure releases through the valves are terminated, such that the radiological doses are within the acceptance limit. The LCO is modified by a Note allowing penetration flow paths with direct access from the containment atmosphere to the outside atmosphere to be unisolated under administrative controls. Administrative controls ensure that 1) appropriate personnel are aware of the open status of the penetration flow path during CORE ALTERATIONS or movement of irradiated fuel assemblies within containment, and 2) specified individuals are designated and readily available to isolate the flow path in the event of a fuel handling accident.

The containment personnel air lock doors may be open during movement of [recently] irradiated fuel in the containment provided that one door is capable of being closed in the event of a fuel handling accident. Should a fuel handling accident occur inside containment, one personnel airlock door will be closed following an evacuations of containment.

APPLICABILITY

The containment penetration requirements are applicable during movement of [recently] irradiated fuel assemblies within containment because this is when there is a potential for the limiting fuel handling accident. In MODES 1, 2, 3, and 4, containment penetration requirements are addressed by LCO 3.6.1, "Containment." In MODES 5 and 6, when movement of irradiated fuel assemblies within containment is not being conducted, the potential for a fuel handling accident does not exist. [Additionally, due to radioactive decay, a fuel handling accident involving handling recently irradiated fuel (i.e., fuel that has occupied part of a critical reactor core within the previous [X] days) will result in doses that are well within the guideline values specified in 10 CFR 100 even without containment closure capability.] Therefore, under these conditions no requirements are placed on containment penetration status.

----------------------------------REVIEWER'S NOTE----------------------------------
The addition of the term "recently" associated with handling irradiated fuel in all of the containment function Technical Specification requirements is only applicable to those licensees who have demonstrated by analysis that after sufficient radioactive decay has occurred, off-site doses resulting from a fuel handling accident remain below the Standard Review Plan limits (well within 10 CFR 100).

BASES

APPLICABILITY (continued)

Additionally, licensees adding the term "recently" must make the following commitment which is consistent with NUMARC 93-01, Revision 4, Section 11.3.6.5 "Safety Assessment for Removal of Equipment from Service During Shutdown Conditions," subheading "Containment - Primary (PWR)/Secondary (BWR)."

"The following guidelines are included in the assessment of systems removed from service during movement of irradiated fuel:

- During fuel handling/core alterations, ventilation system and radiation monitor availability (as defined in NUMARC 91-06) should be assessed, with respect to filtration and monitoring of releases from the fuel. Following shutdown, radioactivity in the fuel decays away fairly rapidly. The basis of the Technical Specification operability amendment is the reduction in doses due to such decay. The goal of maintaining ventilation system and radiation monitor availability is to reduce doses even further below that provided by the natural decay.

- A single normal or contingency method to promptly close primary or secondary containment penetrations should be developed. Such prompt methods need not completely block the penetration or be capable of resisting pressure.

The purpose of the "prompt methods" mentioned above are to enable ventilation systems to draw the release from a postulated fuel handling accident in the proper direction such that it can be treated and monitored."

ACTIONS

A.1 and A.2

With the containment equipment hatch, air locks, or any containment penetration that provides direct access from the containment atmosphere to the outside atmosphere not in the required status, including the Containment Purge and Exhaust Isolation System not capable of automatic actuation when the purge and exhaust valves are open, the unit must be placed in a condition in which the isolation function is not needed. This is accomplished by immediately suspending movement of [recently] irradiated fuel assemblies within containment. Performance of these actions shall not preclude completion of movement of a component to a safe position.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.9.3.1

This Surveillance demonstrates that each of the containment penetrations required to be in its closed position is in that position. The Surveillance on the open purge and exhaust valves will demonstrate that the valves are not blocked from closing. Also, the Surveillance will demonstrate that each valve operator has motive power, which will ensure each valve is capable of being closed by an OPERABLE automatic containment purge and exhaust isolation signal.

The Surveillance is performed every 7 days during movement of [recently] irradiated fuel assemblies within the containment. The Surveillance interval is selected to be commensurate with the normal duration of time to complete fuel handling operations. A surveillance before the start of refueling operations will provide two or three surveillance verifications during the applicable period for this LCO. As such, this Surveillance ensures that a postulated fuel handling accident [involving handling recently irradiated fuel] that releases fission product radioactivity within the containment will not result in a release of significant fission product radioactivity to the environment in excess of those recommended by Standard Review Plan Section 15.7.4 (Ref. 3).

SR 3.9.3.2

This Surveillance demonstrates that each containment purge and exhaust valve actuates to its isolation position on manual initiation or on an actual or simulated high radiation signal. The 18 month Frequency maintains consistency with other similar ESFAS instrumentation and valve testing requirements. In LCO 3.3.4 [(Digital) or 3.3.3 (Analog)], "Miscellaneous Actuations," the Containment Purge Isolation Signal System requires a CHANNEL CHECK every 7 days and a CHANNEL FUNCTIONAL TEST every 31 days to ensure the channel OPERABILITY during refueling operations. Every 18 months a CHANNEL CALIBRATION is performed. The system actuation response time is demonstrated every 18 months, during refueling, on a STAGGERED TEST BASIS. SR 3.6.3.5 demonstrates that the isolation time of each valve is in accordance with the Inservice Testing Program requirements. These surveillances performed during MODE 6 will ensure that the valves are capable of closing after a postulated fuel handling accident [involving handling recently irradiated fuel] to limit a release of fission product radioactivity from the containment.

The SR is modified by a Note stating that this Surveillance is not required to be met for valves in isolated penetrations. The LCO provides the option to close penetrations in lieu of requiring automatic actuation capability.

BASES

REFERENCES	1. GPU Nuclear Safety Evaluation SE-0002000-001, Rev. 0, May 20, 1988.
	2. FSAR, Section [ ].
	3. NUREG-0800, Section 15.7.4, Rev. 1, July 1981.

B 3.9 REFUELING OPERATIONS

B 3.9.4 Shutdown Cooling (SDC) and Coolant Circulation - High Water Level

BASES

BACKGROUND

The purposes of the SDC System in MODE 6 are to remove decay heat and sensible heat from the Reactor Coolant System (RCS), as required by GDC 34, to provide mixing of borated coolant, to provide sufficient coolant circulation to minimize the effects of a boron dilution accident, and to prevent boron stratification (Ref. 1). Heat is removed from the RCS by circulating reactor coolant through the SDC heat exchanger(s), where the heat is transferred to the Component Cooling Water System via the SDC heat exchanger(s). The coolant is then returned to the RCS via the RCS cold leg(s). Operation of the SDC System for normal cooldown or decay heat removal is manually accomplished from the control room. The heat removal rate is adjusted by controlling the flow of reactor coolant through the SDC heat exchanger(s) and bypassing the heat exchanger(s). Mixing of the reactor coolant is maintained by this continuous circulation of reactor coolant through the SDC System.

APPLICABLE SAFETY ANALYSES

If the reactor coolant temperature is not maintained below 200°F, boiling of the reactor coolant could result. This could lead to inadequate cooling of the reactor fuel due to a resulting loss of coolant in the reactor vessel. Additionally, boiling of the reactor coolant could lead to a reduction in boron concentration in the coolant due to the boron plating out on components near the areas of the boiling activity, and because of the possible addition of water to the reactor vessel with a lower boron concentration than is required to keep the reactor subcritical. The loss of reactor coolant and the reduction of boron concentration in the reactor coolant would eventually challenge the integrity of the fuel cladding, which is a fission product barrier. One train of the SDC System is required to be operational in MODE 6, with the water level ≥ 23 ft above the top of the reactor vessel flange, to prevent this challenge. The LCO does permit the SDC pump to be removed from operation for short durations under the condition that the boron concentration is not diluted. This conditional stopping of the SDC pump does not result in a challenge to the fission product barrier.

SDC and Coolant Circulation - High Water Level satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO

Only one SDC loop is required for decay heat removal in MODE 6, with water level ≥ 23 ft above the top of the reactor vessel flange. Only one SDC loop is required because the volume of water above the reactor vessel flange provides backup decay heat removal capability. At least one SDC loop must be OPERABLE and in operation to provide:

a. Removal of decay heat,

b. Mixing of borated coolant to minimize the possibility of a criticality, and

c. Indication of reactor coolant temperature.

An OPERABLE SDC loop includes an SDC pump, a heat exchanger, valves, piping, instruments, and controls to ensure an OPERABLE flow path and to determine the low end temperature. The flow path starts in one of the RCS hot legs and is returned to the RCS cold legs.

Both SDC pumps may be aligned to the Refueling Water Storage Tank to support filing or draining the refueling cavity or for performance of required testing.

The LCO is modified by a Note that allows the required operating SDC loop to be removed from operation for up to 1 hour in each 8 hour period, provided no operations are permitted that would dilute the RCS boron concentration by introduction of coolant into the RCS with boron concentration less than required to meet the minimum boron concentration of LCO 3.9.1. Boron concentration reduction with coolant at boron concentrations less than required to assure the RCS boron concentration is maintained is prohibited because uniform concentration distribution cannot be ensured without forced circulation. This permits operations such as core mapping or alterations in the vicinity of the reactor vessel hot leg nozzles, and RCS to SDC isolation valve testing. During this 1 hour period, decay heat is removed by natural convection to the large mass of water in the refueling cavity.

APPLICABILITY

One SDC loop must be in operation in MODE 6, with the water level ≥ 23 ft above the top of the reactor vessel flange, to provide decay heat removal. The 23 ft level was selected because it corresponds to the 23 ft requirement established for fuel movement in LCO 3.9.6, "Refueling Water Level." Requirements for the SDC System in other MODES are covered by LCOs in Section 3.4, Reactor Coolant System (RCS), and Section 3.5, Emergency Core Cooling Systems (ECCS). SDC loop requirements in MODE 6, with the water level < 23 ft above the top of the reactor vessel flange, are located in LCO 3.9.5, "Shutdown Cooling (SDC) and Coolant Circulation - Low Water Level."

BASES

ACTIONS

SDC loop requirements are met by having one SDC loop OPERABLE and in operation, except as permitted in the Note to the LCO.

A.1

If one required SDC loop is inoperable or not in operation, action shall be immediately initiated and continued until the SDC loop is restored to OPERABLE status and to operation. An immediate Completion Time is necessary for an operator to initiate corrective actions.

A.2

If SDC loop requirements are not met, there will be no forced circulation to provide mixing to establish uniform boron concentrations. Suspending positive reactivity additions that could result in failure to meet the minimum boron concentration limit is required to assure continued safe operation. Introduction of coolant inventory must be from sources that have a boron concentration greater than that what would be required in the RCS for minimum refueling boron concentration. This may result in an overall reduction in RCS boron concentration, but provides acceptable margin to maintaining subcritical operation.

A.3

If SDC loop requirements are not met, actions shall be taken immediately to suspend loading irradiated fuel assemblies in the core. With no forced circulation cooling, decay heat removal from the core occurs by natural convection to the heat sink provided by the water above the core. A minimum refueling water level of 23 ft above the reactor vessel flange provides an adequate available heat sink. Suspending any operation that would increase the decay heat load, such as loading a fuel assembly, is a prudent action under this condition.

A.4, A.5, A.6.1, and A.6.2

If no SDC loop is in operation, the following actions must be taken:

a. The equipment hatch must be closed and secured with [four] bolts,

b. One door in each air lock must be closed, and

BASES

ACTIONS (continued)

c. Each penetration providing direct access from the containment atmosphere to the outside atmosphere must be either closed by a manual or automatic isolation valve, blind flange, or equivalent, or verified to be capable of being closed by an OPERABLE Containment Purge and Exhaust Isolation System.

With SDC loop requirements not met, the potential exists for the coolant to boil and release radioactive gas to the containment atmosphere. Performing the actions described above ensures that all containment penetrations are either closed or can be closed so that the dose limits are not exceeded.

The Completion Time of 4 hours allows fixing of most SDC problems and is reasonable, based on the low probability of the coolant boiling in that time.

SURVEILLANCE REQUIREMENTS

SR 3.9.4.1

This Surveillance demonstrates that the SDC loop is in operation and circulating reactor coolant. The flow rate is determined by the flow rate necessary to provide sufficient decay heat removal capability and to prevent thermal and boron stratification in the core. The Frequency of 12 hours is sufficient, considering the flow, temperature, pump control, and alarm indications available to the operator in the control room for monitoring the SDC System.

REFERENCES

1. FSAR, Section [ ].

B 3.9 REFUELING OPERATIONS

B 3.9.5 Shutdown Cooling (SDC) and Coolant Circulation - Low Water Level

BASES

BACKGROUND

The purposes of the SDC System in MODE 6 are to remove decay heat and sensible heat from the Reactor Coolant System (RCS), as required by GDC 34, to provide mixing of borated coolant, to provide sufficient coolant circulation to minimize the effects of a boron dilution accident, and to prevent boron stratification (Ref. 1). Heat is removed from the RCS by circulating reactor coolant through the SDC heat exchanger(s), where the heat is transferred to the Component Cooling Water System via the SDC heat exchanger(s). The coolant is then returned to the RCS via the RCS cold leg(s). Operation of the SDC System for normal cooldown or decay heat removal is manually accomplished from the control room. The heat removal rate is adjusted by controlling the flow of reactor coolant through the SDC heat exchanger(s) and bypassing the heat exchanger(s). Mixing of the reactor coolant is maintained by this continuous circulation of reactor coolant through the SDC System.

APPLICABLE SAFETY ANALYSES

If the reactor coolant temperature is not maintained below 200°F, boiling of the reactor coolant could result. This could lead to inadequate cooling of the reactor fuel due to the resulting loss of coolant in the reactor vessel. Additionally, boiling of the reactor coolant could lead to a reduction in boron concentration in the coolant due to the boron plating out on components near the areas of the boiling activity, and because of the possible addition of water to the reactor vessel with a lower boron concentration than is required to keep the reactor subcritical. The loss of reactor coolant and the reduction of boron concentration in the reactor coolant would eventually challenge the integrity of the fuel cladding, which is a fission product barrier. Two trains of the SDC System are required to be OPERABLE, and one train is required to be in operation in MODE 6, with the water level < 23 ft above the top of the reactor vessel flange, to prevent this challenge.

SDC and Coolant Circulation - Low Water Level satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

In MODE 6, with the water level < 23 ft above the top of the reactor vessel flange, both SDC loops must be OPERABLE. Additionally, one loop of the SDC System must be in operation in order to provide:

a. Removal of decay heat,

b. Mixing of borated coolant to minimize the possibility of a criticality, and

BASES

LCO (continued)

c. Indication of reactor coolant temperature.

This LCO is modified by two Notes. Note 1 permits the SDC pumps to be removed from operation for ≤ 15 minutes when switching from one train to another. The circumstances for stopping both SDC pumps are to be limited to situations when the outage time is short [and the core outlet temperature is maintained > 10 degrees F below saturation temperature]. The Note prohibits boron dilution by introduction of coolant into the RCS with boron concentration less than that required to meet the minimum boron concentration of LCO 3.9.1, or draining operations when SDC forced flow is stopped.

Note 2 allows one SDC loop to be inoperable for a period of 2 hours provided the other loop is OPERABLE and in operation. Prior to declaring the loop inoperable, consideration should be given to the existing plant configuration. This consideration should include that the core time to boil is short, there is no draining operation to further reduce RCS water level and that the capability exists to inject borated water into the reactor vessel. This permits surveillance tests to be performed on the inoperable loop during a time when these tests are safe and possible.

An OPERABLE SDC loop consists of an SDC pump, a heat exchanger, valves, piping, instruments, and controls to ensure an OPERABLE flow path and to determine the low end temperature. The flow path starts in one of the RCS hot legs and is returned to the RCS cold legs.

Both SDC pumps may be aligned to the Refueling Water Storage Tank to support filling or draining the refueling cavity or for performance of required testing.

APPLICABILITY

Two SDC loops are required to be OPERABLE, and one SDC loop must be in operation in MODE 6, with the water level < 23 ft above the top of the reactor vessel flange, to provide decay heat removal. Requirements for the SDC System in other MODES are covered by LCOs in Section 3.4, Reactor Coolant System. MODE 6 requirements, with a water level ≥ 23 ft above the reactor vessel flange, are covered in LCO 3.9.4, "Shutdown Cooling and Coolant Circulation - High Water Level."

ACTIONS

A.1 and A.2

If one SDC loop is inoperable, action shall be immediately initiated and continued until the SDC loop is restored to OPERABLE status and to operation, or until ≥ 23 ft of water level is established above the reactor vessel flange. When the water level is established at ≥ 23 ft above the

BASES

ACTIONS (continued)

reactor vessel flange, the Applicability will change to that of LCO 3.9.4, "Shutdown Cooling and Coolant Circulation - High Water Level," and only one SDC loop is required to be OPERABLE and in operation. An immediate Completion Time is necessary for an operator to initiate corrective actions.

B.1

If no SDC loop is in operation or no SDC loops are OPERABLE, there will be no forced circulation to provide mixing to establish uniform boron concentrations. Suspending positive reactivity additions that could result in failure to meet the minimum boron concentration limit is required to assure continued safe operation. Introduction of coolant inventory must be from sources that have a boron concentration greater than that what would be required in the RCS for minimum refueling boron concentration. This may result in an overall reduction in RCS boron concentration, but provides acceptable margin to maintaining subcritical operation.

B.2

If no SDC loop is in operation or no SDC loops are OPERABLE, action shall be initiated immediately and continued without interruption to restore one SDC loop to OPERABLE status and operation. Since the unit is in Conditions A and B concurrently, the restoration of two OPERABLE SDC loops and one operating SDC loop should be accomplished expeditiously.

B.3, B.4, B.5.1, and B.5.2

If no SDC loop is in operation, the following actions must be taken:

a. The equipment hatch must be closed and secured with [four] bolts,

b. One door in each air lock must be closed, and

c. Each penetration providing direct access from the containment atmosphere to the outside atmosphere must be either closed by a manual or automatic isolation valve, blind flange, or equivalent, or verified to be capable of being closed by an OPERABLE Containment Purge and Exhaust Isolation System.

.

BASES

ACTIONS (continued)

With SDC loop requirements not met, the potential exists for the coolant to boil and release radioactive gas to the containment atmosphere. Performing the actions stated above ensures that all containment penetrations are either closed or can be closed so that the dose limits are not exceeded.

The Completion Time of 4 hours allows fixing of most SDC problems and is reasonable, based on the low probability of the coolant boiling in that time

SURVEILLANCE REQUIREMENTS

SR 3.9.5.1

This Surveillance demonstrates that one SDC loop is operating and circulating reactor coolant. The flow rate is determined by the flow rate necessary to provide sufficient decay heat removal capability and to prevent thermal and boron stratification in the core. In addition, this Surveillance demonstrates that the other SDC loop is OPERABLE.

In addition, during operation of the SDC loop with the water level in the vicinity of the reactor vessel nozzles, the SDC loop flow rate determination must also consider the SDC pump suction requirements. The Frequency of 12 hours is sufficient, considering the flow, temperature, pump control, and alarm indications available to the operator to monitor the SDC System in the control room.

Verification that the required loops are OPERABLE and in operation ensures that loops can be placed in operation as needed, to maintain decay heat and retain forced circulation. The Frequency of 12 hours is considered reasonable, since other administrative controls are available and have proven to be acceptable by operating experience.

SR 3.9.5.2

Verification that the required pump is OPERABLE ensures that an additional SDC pump can be placed in operation, if needed, to maintain decay heat removal and reactor coolant circulation. Verification is performed by verifying proper breaker alignment and power available to the required pump. The Frequency of 7 days is considered reasonable in view of other administrative controls available and has been shown to be acceptable by operating experience.

REFERENCES

1. FSAR, Section [ ].

B 3.9 REFUELING OPERATIONS

B 3.9.6 Refueling Water Level

BASES

BACKGROUND	The movement of irradiated fuel assemblies within containment requires a minimum water level of 23 ft above the top of the reactor vessel flange. During refueling this maintains sufficient water level in the containment, the refueling canal, the fuel transfer canal, the refueling cavity, and the spent fuel pool. Sufficient water is necessary to retain iodine fission product activity in the water in the event of a fuel handling accident (Refs. 1 and 2). Sufficient iodine activity would be retained to limit offsite doses from the accident to < 25% of 10 CFR 100 limits, as provided by the guidance of Reference 3.
APPLICABLE SAFETY ANALYSES	During movement of irradiated fuel assemblies, the water level in the refueling canal and refueling cavity is an initial condition design parameter in the analysis of the fuel handling accident in containment postulated by Regulatory Guide 1.25 (Ref. 1). A minimum water level of 23 ft (Regulatory Position C.1.c of Ref. 1) allows a decontamination factor of 100 (Regulatory Position C.1.g of Ref. 1) to be used in the accident analysis for iodine. This relates to the assumption that 99% of the total iodine released from the pellet to cladding gap of all the dropped fuel assembly rods is retained by the refueling cavity water. The fuel pellet to cladding gap is assumed to contain 10% of the total fuel rod iodine inventory (Ref. 1). The fuel handling accident analysis inside containment is described in Reference 2. With a minimum water level of 23 ft and a minimum decay time of [X] hours prior to fuel handling, the analysis and test programs demonstrate that the iodine release due to a postulated fuel handling accident is adequately captured by the water and offsite doses are maintained within allowable limits (Ref. 4). Refueling water level satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).
LCO	A minimum refueling water level of 23 ft above the reactor vessel flange is required to ensure that the radiological consequences of a postulated fuel handling accident inside containment are within acceptable limits as provided by the guidance of Reference 3.

BASES

APPLICABILITY	LCO 3.9.6 is applicable when moving fuel assemblies in the presence of irradiated fuel assemblies. The LCO minimizes the possibility of a fuel handling accident in containment that is beyond the assumptions of the safety analysis. If irradiated fuel is not present in containment, there can be no significant radioactivity release as a result of a postulated fuel handling accident. Requirements for fuel handling accidents in the spent fuel pool are covered by LCO 3.7.10, "Fuel Storage Pool Water Level."
ACTIONS	<u>A.1</u> With a water level of < 23 ft above the top of the reactor vessel flange, all operations involving movement of irradiated fuel assemblies shall be suspended immediately to ensure that a fuel handling accident cannot occur. The suspension of fuel movement shall not preclude completion of movement of a component to a safe position.
SURVEILLANCE REQUIREMENTS	<u>SR 3.9.6.1</u> Verification of a minimum water level of 23 ft above the top of the reactor vessel flange ensures that the design basis for the postulated fuel handling accident analysis during refueling operations is met. Water at the required level above the top of the reactor vessel flange limits the consequences of damaged fuel rods that are postulated to result from a fuel handling accident inside containment (Ref. 2). The Frequency of 24 hours is based on engineering judgment and is considered adequate in view of the large volume of water and the normal procedural controls of valve positions, which make significant unplanned level changes unlikely.
REFERENCES	1. Regulatory Guide 1.25, March 23, 1972. 2. FSAR, Section [ ]. 3. NUREG-0800, Section 15.7.4. 4. 10 CFR 100.10.