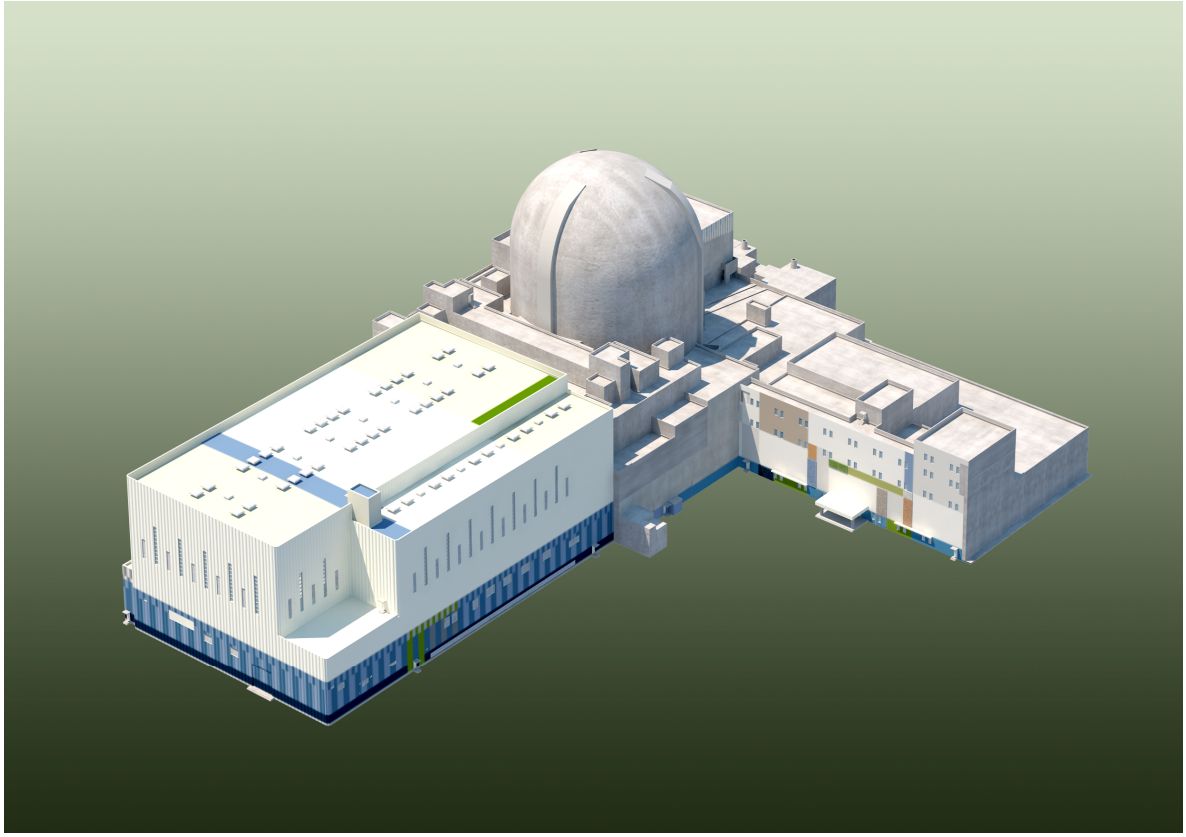
APR1400
DESIGN CONTROL DOCUMENT TIER 2

CHAPTER 16
TECHNICAL SPECIFICATIONS
BASES

APR1400-K-X-FS-13002
REVISION 0
SEPTEMBER 2013



KOREA ELECTRIC POWER CORPORATION
KOREA HYDRO & NUCLEAR POWER CO., LTD

CHAPTER 16 – TECHNICAL SPECIFICATIONS – BASES

TABLE OF CONTENTS

B 2.0 SAFETY LIMITS (SLs)

B 2.1.1 Reactor Core SLs

BASES

BACKGROUND

GDC 10 (Reference 1) requires and SLs ensure that specified acceptable fuel design limits (SAFDLs) 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 having a requirement 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. Overheating of the fuel is prevented by maintaining the steady state peak linear heat rate (LHR) below the level that could cause fuel centerline melting. 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 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 could 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 radioactivity to the reactor coolant.

The reactor protection 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 in LCO 3.3.1 “Reactor Protection System (RPS) Instrumentation – Operating,” 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 DNB 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 (PZR) pressure – High trip

b. PZR pressure – Low trip

c. Variable overpower – High trip

d. Steam generator (SG) pressure – Low trip

e. Local power density (LPD) – High trip

f. DNBR – Low trip

g. SG level – Low trip

h. SG level – High trip

i. Reactor coolant flow – Low trip

j. SG safety valves

BASES

APPLICABLE SAFETY ANALYSES (continued)

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.

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 Reference 2) provide more restrictive limits to ensure that the SLs are not exceeded.

SAFETY LIMITS

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

The minimum value of the DNBR during normal operation and design basis AOOs is limited to 1.29, based on a statistical combination of KCE-1 CHF correlation and engineering factor uncertainties, and is established as an SL. Additional factors (e.g., rod bow, spacer grid size and placement) will determine the limiting safety system settings (LSSS) required to ensure that the SL is maintained. SL 2.1.1.2 ensures that fuel centerline temperature remains below the fuel melt temperature of 5,080 °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 (Reference 3) and adjustments for burnable poisons are established based on Topical Report CENPD-275-P (Reference 4).

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 main steam safety valves (MSSVs) or automatic protection actions serve to prevent RCS heatup to the Reactor Core SL conditions or 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, SLs 2.1.1.1 and 2.1.1.2 are not applicable since the reactor is not generating significant THERMAL POWER.

BASES

SAFETY LIMIT VIOLATIONS

The following 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 is to go to MODE 3 where these SLs are not applicable.

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

REFERENCES

1. 10 CFR 50, Appendix A, GDC 10.
2. DCD Tier 2, Section 15.0.
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, “CE Methodology for Core Designs Containing Gadolinia-Urania Burnable Absorbers,” Revision 1-P-A, May 1988.

B 2.0 SAFETY LIMITS (SLs)

B 2.1.2 Reactor Coolant System (RCS) Pressure SL

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 GDC 14, “Reactor Coolant Pressure Boundary,” and GDC 15, “Reactor Coolant System Design” (Reference 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 (Reference 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 175.8 kg/cm^{2}A (2,500 psia). During normal operation and AOOs, the RCS pressure is kept from exceeding the design pressure by more than 110 %, in accordance with ASME Code, Section III (Reference 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 Section XI (Reference 3), and ASME OM Code (Reference 6).

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 50.34 (Reference 4).

APPLICABLE SAFETY ANALYSES

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

The pressurizer POSRVs are sized to prevent system pressure from exceeding the design pressure by more than 110 %, in accordance with ASME Code, Section III (Reference 2).

BASES

APPLICABLE SAFETY ANALYSES (continued)

The transient that establishes the required relief capacity, and hence the valve size requirements and lift settings, is a complete loss of external load with a delayed 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.

The Reactor Protection System (RPS) trip setpoints, together with the settings of the MSSVs (LCO 3.7.1, “Main Steam Safety Valves (MSSVs)”) and the POSRVs, provide pressure protection for normal operation and AOOs. The Pressurizer Pressure-High trip setpoint is specifically set to provide protection against overpressurization (Reference 5). Safety analyses for both the Pressurizer Pressure-High trip and POSRVs are performed using conservative assumptions relative to pressure control devices. More specifically, no credit is taken for operation of the following:

a. Steam bypass control system

b. Pressurizer level control system

c. Pressurizer pressure control system

d. Feedwater control system

SAFETY LIMITS

The maximum transient pressure allowable in the RCS pressure vessel under the ASME Section III, is 110 % of design pressure. The maximum transient pressure allowable in the RCS piping, valves, and fittings under ASME Code, Section III, is 110 % of design pressure. Therefore, the SL on maximum allowable RCS pressure is 193.3 kg/cm^{2}A (2,750 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 violation responses are applicable to Reactor Core SLs:

2.2.1

If SL 2.1.1.1 or SL 2.1.1.2 is violated, the requirement is to go to MODE 3 where these SLs are not applicable.

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

The following violation responses are applicable to RCS Pressure SL:

2.2.2.1

If SL 2.1.2 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.

If the RCS Pressure SL is exceeded 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 can 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 SL 2.1.2 is violated 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 can be lower and the vessel material, consequently, less ductile. This action does not require reducing mode since this would require reducing temperature, which would compound the problem by adding thermal gradient stresses to the existing pressure stress.

BASES

REFERENCES

1. 10 CFR 50, Appendix A, GDC 14, 15, and 28.
2. ASME Section III, Article NB-7000.
3. ASME Section XI, Article IWX-5000.
4. 10 CFR 50.34.
5. DCD Tier 2, Chapter 15.
6. ASME OM Code.

B 3.0 LIMITING CONDITION FOR OPERATION (LCO) APPLICABILITY

BASES

LCOs	LCO 3.0.1 through LCO 3.0.6 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 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 other conditions exist which 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 Conditions are entered.

LCO 3.0.3

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

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.

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.

BASES

LCO 3.0.3 (continued)

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 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 5 is the next 35 hours, because the total time for reaching MODE 5 is not reduced from the allowable limit of 37 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 3.7.15, “Spent Fuel Pool Water Level.” LCO 3.7.15 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 3.7.15 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 3.7.15 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.

BASES

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 precludes placing the unit in a MODE or other specified condition stated in that Applicability (e.g., Applicability desired to be entered) when the following exist:

a. Unit conditions are such that the requirements of the LCO would not be met in the Applicability desired to be entered; and

b. Continued noncompliance with these LCO requirements, if the Applicability were entered, would result in the unit being required to exit the Applicability desired to be entered to comply with the Required Actions.

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. 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.

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 a normal shutdown.

Exceptions to LCO 3.0.4 are stated in the individual Specifications. Exceptions may apply to all the ACTIONS or to a specific Required Action of a Specification.

LCO 3.0.4 is only applicable when entering MODE 4 from MODE 5, MODE 3 from MODE 4, MODE 2 from MODE 3, or MODE 1 from MODE 2. Furthermore, LCO 3.0.4 is applicable when entering any other specified condition in the Applicability only while operating in MODE 1, 2, 3, or 4. The requirements of LCO 3.0.4 do not apply in MODES 5 and 6, or 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. In some cases these ACTIONS provide a Note that states “While this LCO is not met, entry into a MODE or other specified condition in the Applicability is not permitted, unless required to comply with ACTIONS.” This Note is a requirement explicitly precluding entry into a MODE or other specified condition of the Applicability.

BASES

LCO 3.0.4 (continued)

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, changing MODES or other specified conditions while in an ACTIONS Condition, in compliance with LCO 3.0.4 or where an exception to LCO 3.0.4 is stated, is not a violation of SR 3.0.1 or SR 3.0.4 for those Surveillances that do not have to be performed due to the associated 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 SRs to demonstrate:

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 allowed SRs. This Specification does not provide time to perform any other preventive or corrective maintenance.

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 SRs.

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 an SR 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 an SR on another channel in the same trip system.

BASES

LCO 3.0.6

LCO 3.0.6 establishes an exception to LCO 3.0.2 for support systems that have an 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 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 systems 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 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.

Upon entry into LCO 3.0.6, an evaluation shall be made to determine if loss of safety function exists. Section 4.2 of TS Part 3, "Safety Function Determination Program (SFDP)," ensures loss of safety function is detected and appropriate ACTIONS are taken. 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 systems' Conditions and Required Actions. The SFDP implements the requirements of LCO 3.0.6.

BASES

LCO 3.0.6 (continued)

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).

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.

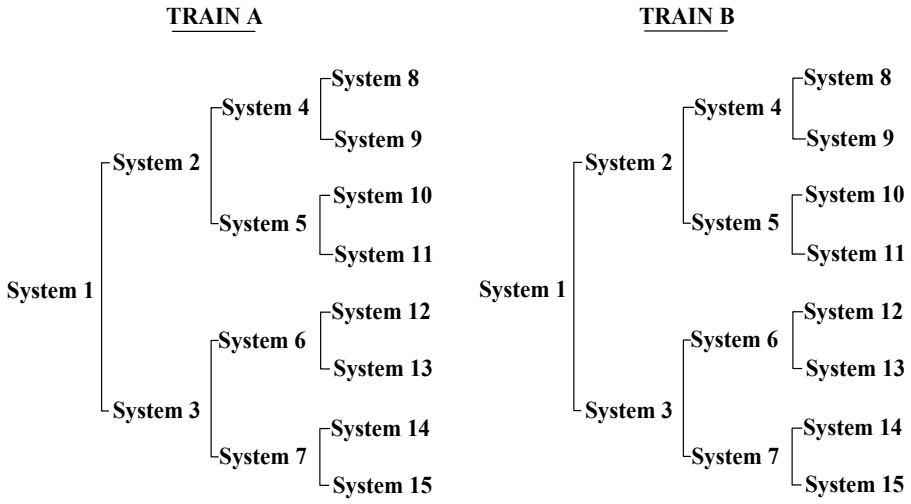


Figure B 3.0-1
Configuration of Trains and Systems

BASES

LCO 3.0.6 (continued)

EXAMPLE B 3.0.6-1

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.

EXAMPLE B 3.0.6-2

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

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.

From the above examples, the left of the supported system is support system (ex, System 1 is the supplement of Systems 2 and 3).

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. 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 apply, in lieu of the ACTIONS of the normal LCO. Exceptions to the above do exist.

BASES

LCO 3.0.7 (continued)

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 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 inoperable.

BASES

LCO 3.0.8 (continued)

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.

LCO 3.0.9

LCO 3.0.9 establishes conditions under which systems described in the TS are considered to remain OPERABLE when required barriers are not capable of providing their related support function(s).

Barriers are doors, walls, floor plugs, curbs, hatches, installed structures or components, or other devices, not explicitly described in TS, that support the performance of the safety function of systems described in the TS. This LCO states that the supported system is not considered to be inoperable solely due to required barriers not capable of performing their related support function(s) under the described conditions. LCO 3.0.9 allows 30 days before declaring the supported system(s) inoperable and the LCO(s) associated with the supported system(s) not met. A maximum time is placed on each use of this allowance to ensure that as required barriers are found or are otherwise made unavailable, they are restored.

BASES

LCO 3.0.9 (continued)

However, the allowable duration may be less than the specified maximum time based on the risk assessment.

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

This provision does not apply to barriers which support ventilation systems or to fire barriers. The TS for ventilation systems provide specific Conditions for inoperable barriers. Fire barriers are addressed by other regulatory requirements and associated plant programs. This provision does not apply to barriers which are not required to support system OPERABILITY (see NRC Regulatory Issue Summary 2001-09, "Control of Hazard Barriers," dated April 2, 2001).

The provisions of LCO 3.0.9 are justified because of the low risk associated with required barriers not being capable of performing their related support function. This provision is based on consideration of the following initiating event categories:

- Loss of coolant accidents
- High energy line breaks
- Feedwater line breaks
- Internal flooding
- External flooding
- Turbine missile ejection
- Tornado or high wind

The provisions of LCO 3.0.9 are justified because of the low risk associated with required barriers not being capable of performing their related support function. This provision is based on consideration of the following initiating event categories:

The risk impact of the barriers which cannot perform their related support function(s) must be addressed pursuant to the risk assessment and management provision of the Maintenance Rule, 10 CFR 50.65 (a)(4), and the associated implementation guidance, NRC RG 1.182, "Assessing and Managing Risk Before Maintenance Activities at Nuclear Power Plants."

BASES

LCO 3.0.9 (continued)

NRC RG 1.182 endorses the guidance in Section 11 of NUMARC 93-01, "Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants."

This guidance provides for the consideration of dynamic plant configuration issues, emergent conditions, and other aspects pertinent to plant operation with the barriers unable to perform their related support function(s). These considerations may result in risk management and other compensatory actions being required during the period that barriers are unable to perform their related support function(s).

LCO 3.0.9 may be applied to one or more trains or subsystems of a system supported by barriers that cannot provide their related support function(s), provided that risk is assessed and managed (including consideration of the effects on Large Early Release and from external events). If applied concurrently to more than one train or subsystem of a multiple train or subsystem supported system, the barriers supporting each of these trains or subsystems must provide their related support function(s) for different categories of initiating events. For example, LCO 3.0.9 may be applied for up to 30 days for more than one train of a multiple train supported system if the affected barrier for one train protects against internal flooding and the affected barrier for the other train protects against tornado missiles. In this example, the affected barrier may be the same physical barrier but serve different protection functions for each train.

If during the time that LCO 3.0.9 is being used, the required OPERABLE train or subsystem becomes inoperable, it must be restored to OPERABLE status within 24 hours. Otherwise, the train(s) or subsystem(s) supported by barriers that cannot perform their related support function(s) must be declared inoperable and the associated LCOs declared not met. This 24-hour period provides time to respond to emergent conditions that would otherwise likely lead to entry into LCO 3.0.3 and a rapid plant shutdown, which is not justified given the low probability of an initiating event which would require the barrier (s) not capable of performing their related support function(s). During this 24 hour period, the plant risk associated with the existing conditions is assessed and managed in accordance with 10 CFR 50.65(a)(4).

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. 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: 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. 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 greater than 56.2 kg/cm^{2}G (800 psig). 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. Safety injection system (SIS) maintenance during shutdown that requires system functional tests at a specified pressure. Provided other appropriate testing is satisfactorily completed, startup can proceed with SIS 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. An example of where SR 3.0.2 does not apply is a Surveillance with a Frequency of "in accordance with 10 CFR 50, Appendix J, as modified by approved exemptions." The requirements of regulations take precedence over the TS. The TS cannot in and of themselves extend a test interval specified in the regulations. Therefore, there is a Note in the Frequency stating, "SR 3.0.2 is not applicable."

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 less, 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 an 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 may 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 or operational situations, is discovered not to have been performed when specified, SR 3.0.3 allows the full delay period of 24 hours to perform the Surveillance.

SR 3.0.3 also provides a time limit for completion 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.

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.

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, train, 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 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. 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 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.

BASES

SR 3.0.4 (continued)

SR 3.0.4 is only applicable when entering MODE 4 from MODE 5, MODE 3 from MODE 4, MODE 2 from MODE 3, or MODE 1 from MODE 2. Furthermore, SR 3.0.4 is applicable when entering any other specified condition in the Applicability only while operating in MODE 1, 2, 3, or 4. The requirements of SR 3.0.4 do not apply in MODES 5 and 6, or 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.

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.1 SHUTDOWN MARGIN (SDM) – T_{cold} > 99 °C (210 °F)

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 (Reference 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 which would be obtained immediately following the insertion of all full strength 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 RCS. The CEA system can compensate for the reactivity effects of the fuel and water temperature changes accompanying power level changes over the range from full load to no load. In addition, the CEAs, together with the boration system, provide the SDM during power operation and are 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 3.1.7, “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.

BASES

APPLICABLE SAFETY ANALYSES

The minimum required SDM is assumed as an initial condition in safety analysis. The safety analysis (Reference 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.

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 for AOOs, and less than or equal to 230 cal/g 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 (Reference 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 will not occur and THERMAL POWER will not violate the safety limit (SL) requirement of SL 2.1.1.

BASES

APPLICABLE SAFETY ANALYSES (continued)

In addition to the limiting MSLB transient, the SDM requirement must also protect against:

a. Inadvertent boron dilution

b. An uncontrolled CEA withdrawal from a subcritical or low power condition

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

d. CEA ejection

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 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.

Depending on the system initial conditions and reactivity insertion rate, the uncontrolled CEA withdrawal transient is terminated by either a low DNBR trip, a high local power density trip, or a Logarithmic Power Level 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.

BASES

APPLICABLE SAFETY ANALYSES (continued)

The CEA ejection is the accident occurring during conditions allowed by the power dependent insertion limit (PDIL). This event will lead to a rapid positive reactivity addition resulting in a rapid power excursion. A reactor trip on high power is generated to terminate the accident. The CEA ejection can result in limited fuel damage with the subsequent release of radioactive material, so it may be necessary to evaluate the radiological consequence in accordance with the 10 CFR 50.34. SDM is an important parameter in this analysis.

In the analysis of the CEA ejection event, SDM alone cannot prevent reactor criticality following a CEA ejection. The k_{N-1} requirement ensures the reactor remains subcritical and, therefore, satisfies the radially averaged enthalpy acceptance criterion considering power redistribution effects.

The function of k_{N-1} is to maintain sufficient subcriticality to preclude inadvertent criticality following ejection of a single control element assembly (CEA). k_{N-1} is a measure of the core's reactivity, considering a single malfunction resulting in the highest worth inserted CEA being ejected.

k_{N-1} requirements vary with the amount of positive reactivity that would be introduced assuming the CEA with the highest inserted worth ejects from the core. The k_{N-1} requirement ensures that a CEA ejection event while shutdown will not result in criticality.

The requirement prohibiting criticality due to shutdown group CEA movement is associated with the assumptions used in the analysis of uncontrolled CEA withdrawal from subcritical conditions. Due to the high differential reactivity worth of the shutdown CEA groups, the analysis assumes that the initial shutdown reactivity is such that the reactor will remain subcritical in the event of unexpected or uncontrolled shutdown group withdrawal.

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

LCO

The MSLB accident (Reference 2) and the boron dilution accident (Reference 3) 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 50.34 limits (Reference 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, k_{N-1}, and criticality due to shutdown CEA withdrawal are a core physics design condition that can be ensured through CEA positioning (regulating and shutdown CEAs) and through the soluble boron concentration.

BASES

APPLICABILITY

In MODES 3 and 4, 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 3.1.6, "Shutdown Control Element Assembly (CEA) Insertion Limits," and LCO 3.1.7 "Regulating Control Element Assembly (CEA) Insertion Limits." If the insertion limits of LCO 3.1.6 or LCO 3.1.7 are not being complied with, SDM is not automatically violated. The SDM must be calculated by performing a reactivity balance calculation (considering the listed reactivity effects in Bases Section SR 3.1.1.1).

In MODE 5, the shutdown reactivity requirements are given in LCO 3.1.2, "SHUTDOWN MARGIN (SDM) – T_{cold} ≤ 99 °C (210 °F)." 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 (above 4,000 ppm boric acid and 109.8 L/min (29 gpm) flow rate), the boron concentration should be a highly concentrated solution, such as boric acid in the IRWST. The operator should borate with the best source available for the plant conditions.

B.1 and B.2

If the k_{N-1} requirements are not met or reactor criticality is achievable by Shutdown Group CEA movement, boration must be initiated promptly and CEA position varied to restore k_{N-1} within limit or to ensure criticality due to Shutdown Group CEA movement is not achievable. A Completion Time of 15 minutes is adequate for an operator to correctly align and start the required systems and components and vary CEA position. It is assumed that boration will be continued and CEA position varied to return k_{N-1} to within limit or prevent reactor criticality due to Shutdown Group CEA movement. CEA movement is only required if the specific limit exceeded can be improved by taking this action.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.1.1.1, 3.1.1.2, 3.1.1.3

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

a. RCS boron concentration

b. CEA positions

c. RCS cold leg temperature

d. Fuel burnup based on gross thermal energy generation

e. Xenon concentration

f. Samarium concentration

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 that of the RCS.

The Frequency of 24 hours is based on the generally slow change in required boron concentration, and it 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. DCD Tier 2, Subsection 15.1.5.

3. DCD Tier 2, Subsection 15.4.6.

4. 10 CFR 50.34.

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.2 SHUTDOWN MARGIN (SDM) – T_{cold} ≤ 99 °C (210 °F)

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 (Reference 1). Maintenance of the 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 which would be obtained immediately following the insertion of all full strength 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 can compensate for the reactivity effects of the fuel and water temperature changes accompanying power level changes over the range from full load to no load. In addition, the CEAs, together with the boration system, provide the SDM during power operation and are 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. SDM is defined as the reactivity of the core with all CEAs inserted, 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 3.1.7, “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.

BASES

APPLICABLE SAFETY ANALYSES

The minimum required SDM is assumed as an initial condition in safety analysis. The safety analysis (Reference 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.

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 for AOOs, and less than or equal to 230 cal/g energy deposition for the CEA ejection accident); and

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

An inadvertent boron dilution is a moderate Frequency incident as defined in Reference 2. The core is initially subcritical with all CEAs inserted. A chemical and volume control system (CVCS) malfunction occurs which causes unborated water to be pumped to the RCS via one charging pump.

The reactivity change rate associated with boron concentration changes due to inadvertent dilution is within the capabilities of operator recognition and control. The high neutron flux alarm on the startup channel instrumentation will alert the operator of the boron dilution with a minimum of 30 minutes remaining before the core becomes critical.

SDM satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii). Even though it is not directly observed from the MCR, SDM is considered an initial condition process variable because it is periodically monitored to ensure that the unit is operating within the bounds of the accident analysis assumptions.

In the analysis of the CEA ejection event, SDM alone cannot prevent reactor criticality following a CEA ejection. The k_{N-1} requirement ensures the reactor remains subcritical and, therefore, satisfies the radially averaged enthalpy acceptance criterion considering power redistribution effects.

BASES

APPLICABLE SAFETY ANALYSES (continued)

The function of k_{N-1} is to maintain sufficient subcriticality to preclude inadvertent criticality following ejection of a single control element assembly (CEA). k_{N-1} is a measure of the core's reactivity, considering a single malfunction resulting in the highest worth inserted CEA being ejected.

k_{N-1} requirements vary with the amount of positive reactivity that would be introduced assuming the CEA with the highest inserted worth ejects from the core. The k_{N-1} requirement ensures that a CEA ejection event while shutdown will not result in criticality.

The requirement prohibiting criticality due to shutdown group CEA movement is associated with the assumptions used in the analysis of uncontrolled CEA withdrawal from subcritical conditions. Due to the high differential reactivity worth of the shutdown CEA groups, the analysis assumes that the initial shutdown reactivity is such that the reactor will remain subcritical in the event of unexpected or uncontrolled shutdown group withdrawal.

LCO

Chapter 15 accident analyses have shown that the required SDM is sufficient to avoid unacceptable consequences to the fuel or RCS as a result of the events addressed above.

The most limiting accident for the SDM requirements in MODE 5 is based on a boron dilution accident as described in the accident analysis (Reference 2). 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, k_{N-1}, and criticality due to shutdown CEA withdrawal are a core physics design condition that can be ensured through CEA positioning (regulating and shutdown CEAs) and through the soluble boron concentration.

APPLICABILITY

In MODE 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 3.1.6, “Shutdown Control Element Assembly (CEA) Insertion Limits,” and LCO 3.1.7 “Regulating Control Element Assembly (CEA) Insertion Limits.” If the insertion limits of LCO 3.1.6 or LCO 3.1.7 are not being complied with, SDM is not automatically violated. The SDM must be calculated by performing a reactivity balance calculation (considering the listed reactivity effects in Bases Section SR 3.1.2.1).

In MODE 3 and 4, the shutdown reactivity requirements are given in LCO 3.1.1 “SHUTDOWN MARGIN (SDM) – T_{cold} > 99 °C (210 °F).” In MODE 6, the shutdown reactivity requirements are given in LCO 3.9.1, “Boron Concentration.”

BASES

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. The operator should borate with the best source available for the plant conditions.

Since it is imperative to raise the boron concentration of the RCS as soon as possible (above 4,000 ppm boric acid and 109.8 L/min (29 gpm) flow rate), the boron concentration should be a highly concentrated solution, such as boric acid in the IRWST. The operator should borate with the best source available for the plant conditions.

B.1 and B.2

If the k_{N-1} requirements are not met or reactor criticality is achievable by Shutdown Group CEA movement, boration must be initiated promptly and CEA position varied to restore k_{N-1} within limit or to ensure criticality due to Shutdown Group CEA movement is not achievable. A Completion Time of 15 minutes is adequate for an operator to correctly align and start the required systems and components and vary CEA position. It is assumed that boration will be continued and CEA position varied to return k_{N-1} to within limit or prevent reactor criticality due to Shutdown Group CEA movement. CEA movement is only required if the specific limit exceeded can be improved by taking this action.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.1.2.1, 3.1.2.2, 3.1.2.3

In MODE 5, SDM is verified by performing a reactivity balance calculation, considering the listed reactivity effects:

a. RCS boron concentration

b. CEA positions

c. RCS cold leg temperature

d. Fuel burnup based on gross thermal energy generation

e. Xenon concentration

f. Samarium concentration

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 that of the RCS.

The Frequency of 24 hours is based on the generally slow change in required boron concentration, and it 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. DCD Tier 2, Subsection 15.4.6.

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.3 Reactivity Balance

BASES

BACKGROUND

According to GDC 26, 28, and 29 (Reference 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 accidents (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) – T_{cold} > 99 °C (210 °F)”) 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.

BASES

BACKGROUND (continued)

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.

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 (Reference 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.

BASES

APPLICABLE SAFETY ANALYSES (continued)

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.

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 the predicted value 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.

BASES

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, CEA replacement, shuffling).

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.

BASES

ACTIONS (continued)

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

B.1

If the core reactivity cannot be restored to within the ± 1 % $\Delta k/k$ of predicted values, 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.

SURVEILLANCE REQUIREMENTS

SR 3.1.3.1

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 two 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 3.1.3.1 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, 28, and 29.

2. DCD Tier 2, Chapter 15.

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.4 Moderator Temperature Coefficient (MTC)

BASES

BACKGROUND

According to GDC 11 (Reference 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 non-positive MTC throughout the 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.

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 distributed absorber (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 (Reference 2).

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 (Reference 2).

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 (Reference 2).

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 main steam line break (MSLB) event. Following the reactor trip for the postulated EOC MSLB 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 3.1.4 requires the MTC to be within the positive and negative limits specified in 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 positive MTC limit 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.

The MTC limit specified in the LCO is the maximum positive MTC value approved in the plant's licensing basis and ensures that the reactor operates with a negative MTC over the largest possible range of fuel cycle operation. The cycle-specific MTC limit specified in the COLR must be equal to or less positive than the MTC limit specified in the LCO.

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. Limited control of MTC can be achieved by adjusting CEA position and boron concentration. During operation the LCO can be ensured through measurement and adjustments to CEA position and boron concentration. 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.

BASES

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.

SURVEILLANCE REQUIREMENTS

SR 3.1.4.1 and SR 3.1.4.2

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 greater than 5 % RTP satisfies the confirmatory check on the most positive (least negative) MTC value.

The requirement for measurement, within 7 EFPD after reaching 40 EFPD and 2/3 of 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 can be evaluated before the reactor actually reaches the EOC condition. MTC values can be extrapolated and compensated to permit direct comparison to the specified MTC limits.

SR 3.1.4.2 is modified by a Note that indicates, if extrapolated MTC is more negative than the EOC limit specified in the COLR, 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. DCD Tier 2, Section 15.0.

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.5 Control Element Assembly (CEA) Alignment

BASES

BACKGROUND

The OPERABILITY (e.g., trippability) of the shutdown and regulating CEAs are initial assumptions in all safety analyses, which assume CEA insertion upon reactor trip. Maximum CEA misalignment is an initial assumption in the safety analyses which 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 26 (Reference 1), and 10 CFR 50.46 (Reference 2).

Mechanical or electrical failures can cause a CEA to become inoperable or to become misaligned from its group. CEA inoperability or misalignment can 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 1.91 cm (3/4 in)) at a time, but at varying rates (steps per minute) depending on the signal output from the digital rod control system (DRCS).

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 can be automatically controlled by the reactor regulating system (RRS).

Part strength CEAs are not credited in the safety analyses for shutting down the reactor, as are the regulating and shutdown groups. The part strength CEAs are used for Axial Shape Index (ASI) control.

BASES

BACKGROUND (continued)

The axial positions of shutdown and regulating CEAs are indicated by two separate and independent systems. These 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 DRCS 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 1.91 cm (± 3/4 in)). 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 3.81 cm (1.5 in), 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 (Reference 3). The accident analysis defines CEA misoperation as any event, with the exception of sequential group withdrawals, that could result from a single malfunction in the reactivity control systems. For example, CEA misalignment can be caused by a malfunction of the CEDM, DRCS, or by operator error. A stuck CEA can be caused by mechanical jamming of the CEA fingers or the gripper. Inadvertent withdrawal of a single CEA can be caused by opening of the electrical circuit of the CEDM holding coil for a full strength or part strength 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 (SAFDL) 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 can 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 can result in excessive local linear heat rates (LHRs).

Two types of analyses are performed in regard to static CEA misalignment (Reference 3). With CEA banks at their insertion limits, one type of analysis considers the case when any one CEA is inserted fully into the core. The second type of analysis considers the case of a single CEA withdrawn 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 16.8 cm (6.6 in).

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 (Reference 3).

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 SAFDLs are approached.

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 strength CEA drop, a single part strength CEA drop, and a single part strength CEA subgroup drop. The most rapid approach to the DNBR SAFDL can be caused by either a single full strength drop or a part strength CEA subgroup drop depending upon initial conditions. The most rapid approach to the fuel centerline melt SAFDL is caused by a single part strength CEA drop.

BASES

APPLICABLE SAFETY ANALYSES (continued)

In the case of the full strength 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 strength CEA subgroup drop, a distortion in power distribution, and a decrease in core power are produced. As the dropped part strength 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 strength CEA drop, both core average power and three dimensional peak to average power density increase promptly. As the dropped part strength 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 that ensure 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.

The requirement on OPERABILITY to maintain the CEA alignment to within 16.8 cm (6.6 in) between the highest and lowest CEAs in a subgroup is conservative. The minimum misalignment assumed in safety analysis is 48.3 cm (19 in), and in some cases, a total misalignment from fully withdrawn to fully inserted is assumed.

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

BASES

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) – T_{cold} > 99 °C (210 °F)” and LCO 3.1.2, “SHUTDOWN MARGIN (SDM) – T_{cold} ≤ 99 °C (210 °F)” for SDM in MODES 3, 4, and 5, and LCO 3.9.1 “Boron Concentration,” for boron concentration requirements during refueling.

ACTIONS

A.1, A.2.1, A.2.2, A.3.1, and A.3.2

A CEA can become misaligned, yet remain trippable. In this condition, the CEA can still perform its required function of adding negative reactivity should a reactor trip be necessary.

If one or more regulating CEAs are misaligned by greater than 16.8 cm (6.6 in) and less than or equal to 48.3 cm (19 in) but trippable, or one regulating CEA misaligned by greater than 48.3 cm (19 in) but trippable, continued operation in MODES 1 and 2 may continue provided, within 1 hour, the power is reduced in accordance with Figure 3.1.5-1 and SDM is within the limit specified in the COLR or boration is initiated to restore SDM to within limits, and within 2 hours the misaligned CEA(s) is aligned within 16.8 cm (6.6 in) of its group or the misaligned CEA's group is aligned within 16.8 cm (6.6 in) of the misaligned CEA(s).

Xenon redistribution in the core starts to occur as soon as a CEA becomes misaligned. Reducing THERMAL POWER in accordance with Figure 3.1.5-1 (in the accompanying LCO) ensures acceptable power distributions are maintained (Reference 3). For small misalignments (less than 48.3 cm (19 in)) 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

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

BASES

ACTIONS (continued)

With a large CEA misalignment (greater than or equal to 48.3 cm (19 in)), however, this misalignment would cause distortion of the core power distribution. This distortion can, in turn, have a significant effect on:

a. The available SDM

b. The time dependent, long term power distributions relative to those used in generating LCOs and LSSS setpoints

c. The ejected CEA worth used in the accident analysis

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 the cause of a misaligned CEA.

b. Take appropriate corrective action to realign the CEAs.

c. Minimize the effects of xenon redistribution.

In this condition, an additional allowance must be made for the worth of the affected CEA when calculating the available SDM. With one or more misaligned CEAs, SDM must be verified for CEAs at the existing nonaligned positions. SDM is calculated by performing a reactivity balance calculation according to procedure, considering the listed effects in SR 3.1.1.1. This is necessary since the OPERABLE CEAs must still meet the single failure criterion. If additional negative reactivity is required to provide the necessary SDM, it must be provided by increasing the RCS boron concentration. One hour allows sufficient time to perform the SDM calculation and make any required boron adjustment to the RCS.

B.1, B.2.1, B.2.2, and B.3

If one or more shutdown CEAs are misaligned by greater than 16.8 cm (6.6 in) and less than or equal to 48.3 cm (19 in) but trippable, or one shutdown CEA misaligned by greater than 48.3 cm (19 in) but trippable, continued operation in MODES 1 and 2 may continue provided, within 1 hour, the power is reduced in accordance with Figure 3.1.5-1 and SDM is within the limit specified in the COLR to restore SDM to within limits, and within 2 hours the misaligned CEA(s) is aligned within 16.8 cm (6.6 in) of its group.

BASES

ACTIONS (continued)

C.1, C.2.1, and C.2.2

If one or more part strength CEAs are misaligned by greater than 16.8 cm (6.6 in) and less than or equal to 48.3 cm (19 in) or one part strength CEA misaligned by greater than 48.3 cm (19 in), continued operation in MODES 1 and 2 may continue provided power is reduced in accordance with Figure 3.1.5-1 within 1 hour and within 2 hours the misaligned CEA(s) is restored to within 16.8 cm (6.6 in) of its group, or the misaligned CEA's group is aligned within 16.8 cm (6.6 in) of the misaligned CEA.

Although a part strength CEA has less of an effect on core flux than a full strength CEA, a misaligned part strength CEA will still result in xenon redistribution and affect core power distribution.

Requiring realignment within 2 hours minimizes these effects and ensures acceptable power distribution is maintained.

D.1

If a Required Action or associated Completion Time of Condition A, Condition B, or Condition C is not met, one or full strength CEAs are untrippable, or two or more CEAs are misaligned by greater than 48.3 cm (19 in), 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. 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. 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 3.1.6, “Shutdown Control Element Assembly (CEA) Insertion Limits,” and LCO 3.1.7, “Regulating Control Element Assembly (CEA) Insertion Limits,” does not ensure that adequate SDM exists. Therefore, the plant must be shut down in order to evaluate the SDM required boron concentration and power level for critical operation.

Continued operation is not allowed in the case of more than one CEA(s) misaligned from any other CEA in its group by greater than 48.3 cm (19 in), or with one or more full strength CEAs untrippable. This is because these cases are indicative of a loss of SDM and power distribution, and a loss of safety function, respectively.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.1.5.1

Verification that individual CEA positions are within 16.8 cm (6.6 in) (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 12-hour Frequency takes into account other CEA position information that is continuously available to the operator in the MCR, so that during actual CEA motion, deviations can immediately be detected.

SR 3.1.5.2

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. The specified 12-hour Frequency takes into account other CEA position information that is continuously available to the operator in the MCR, so that during actual CEA motion, deviations can immediately be detected.

SR 3.1.5.3

Verifying each full strength CEA is trippable would require that each CEA be tripped. In MODES 1 and 2 tripping each full strength CEA would result in radial or axial power tilts, or oscillations. Therefore individual full strength CEAs are exercised every 92 days to provide increased confidence that all full strength CEAs continue to be trippable, even if they are not regularly tripped. A movement of 12.7 cm (5 in) is adequate to demonstrate motion without exceeding the alignment limit when only one full strength CEA is being moved. The 92-day Frequency takes into consideration other information available to the operator in the MCR and other Surveillances being performed more frequently, which add to the determination of OPERABILITY of the CEAs (Reference 3). Between required performances of SR 3.1.5.3, if a CEA(s) is discovered to be immovable but remains trippable and aligned, the CEA is considered to be OPERABLE. At any time, if a CEA(s) is immovable, a determination of the trippability (OPERABILITY) of that CEA(s) must be made and appropriate action taken.

SR 3.1.5.4

Performance of a CHANNEL FUNCTIONAL TEST of each reed switch position transmitter (RSPT) channel ensures the channel is OPERABLE and capable of indicating CEA position. 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.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.1.5.5

Verification of full strength CEA drop times determines that the maximum CEA drop time permitted is consistent with the assumed drop time used in the safety analysis (Reference 3). 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.

The 4 second CEA drop time is the maximum time it takes for a fully withdrawn individual full strength CEA to reach its 90% insertion position when electrical power is interrupted to the CEA drive mechanism with RCS Tcold greater than or equal to [286.7 °C (548 °F)] and all reactor coolant pumps operating. The CEA drop time of full strength CEAs shall also be demonstrated through measurement prior to reactor criticality for specifically affected individual CEAs following any maintenance on or modification to the CEA drive system which could affect the drop time of those specific CEAs.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 10 and 26.
2. 10 CFR 50.46.
3. DCD Tier 2, Section 15.4.

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.6 Shutdown Control Element Assembly (CEA) Insertion Limits

BASES

BACKGROUND

The insertion limits of the shutdown 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 and 26 (Reference 1), and 10 CFR 50.46 (Reference 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 MCR 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.

BASES

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.

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

CEAs are considered fully withdrawn at 367.7 cm (144.75 in) since this position places them outside the active region of the core.

On a reactor trip, all CEAs (shutdown 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 3.1.7, "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) – T_{cold} > 99 °C (210 °F)") 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 maintain the required SDM at rated no load temperature (Reference 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:

1. Specified acceptable fuel design limits(SAFDL)

2. Reactor coolant system (RCS) pressure boundary integrity

b. The core remains subcritical after accident transients.

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

BASES

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.

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 MODES 1 and 2, if shutdown CEAs are not within their insertion limits, then SDM will be verified by performing a reactivity balance calculation (considering the listed reactivity effects in bases section SR 3.1.1.1).

In MODE 3, 4, 5, and 6, the shutdown CEAs are fully inserted in the core and contribute to the SDM. Refer to LCO 3.1.1 “SHUTDOWN MARGIN (SDM) – T_{cold} > 99 °C (210 °F)” and LCO 3.1.2 “SHUTDOWN MARGIN (SDM) – T_{cold} ≤ 99 °C (210 °F)” for SDM requirements in MODES 3, 4, and 5. LCO 3.9.1, “Boron Concentration,” ensures adequate SDM in MODE 6.

LCO 3.1.6 has been modified by a Note indicating the LCO requirement is suspended during SR 3.1.5.3, 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.1.1, A.1.2, and A.2

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 boron concentration is not changed at this time, SDM should not change. This, however, is verified within 1 hour, or boration is initiated to bring the SDM to within limit, if the CEA(s) is not restored to within limits prior to this time.

If the CEA(s) is not restored to within limits within 1 hour and the SDM is within limit, 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 3.1.5, “Control Element Assembly (CEA) Alignment.”

BASES

ACTIONS (continued)

B.1

When Required Action A.1.1, A.1.2, 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.

SURVEILLANCE REQUIREMENTS

SR 3.1.6.1

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.

Since the shutdown CEAs are positioned manually by the main control room (MCR) 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 MCR for the purpose of monitoring the status of the shutdown CEAs.

A NOTE in FREQUENCY column always assures that required SDM is maintained by verifying each shutdown CEA is withdrawn greater than or equal to 367.7 cm (144.75 in) (SR 3.1.6.1) within 15 minutes prior to withdrawal of any CEA in regulating groups during an approach to reactor criticality.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 10 and 26.
2. 10 CFR 50.46.
3. DCD Tier 2, Section 15.0.

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.7 Regulating Control Element Assembly (CEA) Insertion Limits

BASES

BACKGROUND

The insertion limits of the regulating 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 GDC 10 and 26 (Reference 1) and 10 CFR 50.46 (Reference 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 (Reference 2). Together, 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 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 (F_{xy}),” 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 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_{xy}, 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.

BASES

BACKGROUND (continued)

The establishment of limiting safety system settings (LSSS) 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 (NSSS) (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 3.1.7 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 AZIMUTHAL POWER TILT (T_q), are process variables that 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 strength 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 1,204 °C (2,200 °F) per 10 CFR 50.46 (Reference 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 rod 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 230 cal/g (Reference 3).

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

Regulating CEA position, ASI, and T_q are process variables that 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 (Reference 3).

BASES

APPLICABLE SAFETY ANALYSES (continued)

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). However, the most limiting SDM requirements for MODES 1 and 2 at EOC come from the 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.

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, adherence to LCOs 3.1.6 and 3.1.7 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 or ASI limits can approach the maximum allowable linear heat generation rate or peaking factor, with the allowed T_q present. Operation at the insertion limit can 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 (Reference 3).

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

BASES

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.

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 3.1.5.3. 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.

BASES

ACTIONS

A.1.1, A.1.2, A.2.1, and A.2.2

Operation beyond the transient insertion limit can result in a loss of SDM and excessive peaking factors. If the regulating CEA insertion limits are not met, then SDM must be verified by performing a reactivity balance calculation, considering the listed reactivity effects in bases section SR 3.1.1.1. One hour is sufficient time for conducting the calculation and commencing boration if the SDM is not within limits. The transient insertion limit should not be violated during normal operation; this violation, however, can 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 greater than 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 (Reference 3).

Additionally, since the CEAs can be in this condition without misalignment, penalty factors are not inserted in the core protection calculators (CPCs) 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.

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 less than or equal 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 (Reference 3).

BASES

ACTIONS (continued)

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 EFPD or 14 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.1.1, D.1.2, D.2.1, and D.2.2

If the regulating CEA insertion limits are not met, then SDM must be verified by performing a reactivity balance calculation, considering the effects in SR 3.1.1.1 Bases. One hour is sufficient time for conducting the calculation and commencing boration if the SDM is not within limits. With the Core Operating Limit Supervisory System (COLSS) 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 (Reference 3). 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.

E.1

With the PDIL circuit inoperable, performing SR 3.1.7.1 within 1 hour and every 4 hours thereafter ensures improper CEA alignments are identified before unacceptable flux distributions occur.

BASES

ACTIONS (continued)

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 3.1.7.1

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 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 MCR.

SR 3.1.7.1 is modified by a Note indicating that this Surveillance is not required prior to entry into MODE 2. 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 3.1.7.2

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 3.1.7.3

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 26.
2. 10 CFR 50.46.
3. DCD Tier 2, Section 15.4.

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.8 Part Strength Control Element Assembly (CEA) Insertion Limits

BASES

BACKGROUND

The insertion limits of the part strength 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 GDC 10 (Reference 1) and 10 CFR 50.46 (Reference 2). Limits on part strength 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 (SAFDL), including limits that preserve the criteria specified in 10 CFR 50.46 (Reference 2). Together, LCO 3.1.7, “Regulating Control Element Assembly (CEA) Insertion Limits,” LCO 3.1.8, 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 System 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.

BASES

BACKGROUND (continued)

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 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 (e.g., base loaded, maneuvering). 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 3.1.8 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 strength 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 1,204 °C (2,200 °F) per 10 CFR 50.46 (Reference 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 rod 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 230 cal/g (Reference 3).

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

BASES

APPLICABLE SAFETY ANALYSES (continued)

Regulating CEA position, part strength CEA position, ASI, and T_q are process variables that 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 part strength CEA insertion limits satisfy Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

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

APPLICABILITY

The part strength insertion limits shall be maintained with the reactor in MODE 1 greater than 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 strength CEAs. Exercising part strength CEAs could require moving them outside their insertion limits.

ACTIONS

A.1

If the part strength 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 could be invalidated (Reference 3).

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.

BASES

ACTIONS (continued)

Since these effects are cumulative, ACTIONS are provided to limit the total time the part strength 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 strength CEAs to within the allowed limits.

B.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 less than or equal to 20 % RTP from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.1.8.1

Verification of each part strength CEA group position every 12 hours is sufficient to detect CEA positions that could 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 MCR.

SR 3.1.8.2

Verification of the accumulated time of part strength CEA group insertion beyond the long term steady state 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.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 10 and 26.
2. 10 CFR 50.46.
3. DCD Tier 2, Section 15.4.

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.9 Charging Flow

BASES

BACKGROUND	Charging flow restriction orifice is a component for the protection of an excessive charging flow from the CVCS into the RCS when RCS pressure is low. This component is for the confirmation of an assumption of initial condition for safety analysis of inadvertent deboration event to prevent excessive unborated charging water to the RCS during MID-LOOP operation in MODE 5.
APPLICABLE SAFETY ANALYSES	Charging flow restriction during MODE 5 (MID-LOOP operation) is an assumption of initial condition for safety analysis of inadvertent deboration event as described in the DCD TIER 2 (Reference 1). During MID-LOOP operation, charging flow restriction is achievable by closing orifice bypass valve and removing the power to the above valve, and it satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).
LCO	The LCO requires that a charging flow shall be restricted during MID-LOOP operation in MODE 5 by closing charging flow restriction orifice bypass valve and removing the power to the above valve.
APPLICABILITY	The LCO is applicable during MODE 5 (MID-LOOP operation). Charging flow restriction condition shall be met during MODE 5 (MID-LOOP operation) since a charging flow is assumed to be less than 567.8 L/min (150 gpm) for safety analysis of inadvertent deboration event during MID-LOOP operation.
ACTIONS	A.1 Turn off charging pump immediately to prohibit a possible excessive positive reactivity addition if LCO 3.1.9 is not met. But, an auxiliary charging pump, which supplies a restricted charging flow, may be turned on if necessary. A.2 To ensure a SHUTDOWN MARGIN without a charging pump turnoff, suspend all operations immediately involving positive reactivity changes under the operator's control, if LCO 3.1.9 is not met.

BASES

SURVEILLANCE REQUIREMENTS	SR 3.1.9.1 By verifying that the charging flow restriction orifice bypass valves are closed and the power to the above valves is removed, a possible positive reactivity addition into the RCS can be restricted. The 8-hour Frequency for this Surveillance is enough to verify that orifice valve is closed and the power to the above valves is removed.
REFERENCES	1. DCD Tier 2, Section 15.4.

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.10 Special Test Exceptions (STE) – SHUTDOWN MARGIN (SDM)

BASES

BACKGROUND

The primary purpose of the SDM 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 and SDM.

10 CFR 50, Appendix B, Section XI (Reference 1) requires that a test program be established to ensure that structures, systems, and components (SSCs) will perform satisfactorily in service. All functions necessary to ensure that specified design conditions are not exceeded during normal operation and anticipated operational occurrences (AOOs) 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" (Reference 2).

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

a. Ensure facility has been adequately designed.

b. Validate analytical models used in design and analysis.

c. Verify assumptions used for predicting plant response.

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

e. Verify 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 the initial core and 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 (Reference 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 the design intent is met.

BASES

BACKGROUND (continued)

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 as long as 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-19.6.1-1997 (Reference 4). PHYSICS TESTS for reload fuel cycles are given in Table 1 of ANSI/ANS-19.6.1-1997. Although these PHYSICS TESTS are generally accomplished within the limits of all LCOs, conditions could 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) and the departure from nucleate boiling ratio (DNBR) remain within their limits, fuel design criteria are preserved.

In this test, the following LCOs are suspended:

a. LCO 3.1.1, “SHUTDOWN MARGIN (SDM): T_{cold} > 99 °C (210 °F)”

b. LCO 3.1.6, “Shutdown Control Element Assembly (CEA) Insertion Limits”

c. LCO 3.1.7, “Regulating Control Element Assembly (CEA) Insertion Limits”

d. LCO 3.3.1, “Reactor Protection System (RPS) Instrumentation – Operating” (Only applied to Trip Functions 2, 14 and 15 in Table 3.3.1-1)

e. LCO 3.3.2, “Reactor Protection System (RPS) Instrumentation – Shutdown” (Only Applied to Trip Function 1 in Table 3.3.2-1).

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.

BASES

APPLICABLE SAFETY ANALYSES (continued)

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 Tc, and pressurizer pressure contribute to maintaining DNBR limits. The initial condition criteria for accidents sensitive to core power distribution are preserved by the LHR and DNBR limits. The criteria for the loss-of-coolant accident (LOCA) are specified in 10 CFR 50.46 (Reference 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 DNBR limits preserves the loss of flow criteria.

SRs are conducted as necessary to ensure that LHR and DNBR 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, withdrawal of each tripped CEA within 24 hours prior to suspending the SDM requirements, and ensuring that shutdown reactivity is available equivalent to the reactivity worth of the estimated highest worth withdrawn CEA (Reference 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 in their respective LCOs.

BASES

APPLICABLE SAFETY ANALYSES (continued)

As described in LCO 3.0.7, compliance with Special Test Exception (STE) LCOs is optional, and therefore no SECTION CRITERIA apply. STE LCOs provide flexibility to perform certain operations by appropriately modifying requirements of other LCOs. A discussion of the SELECTION CRITERIA satisfied for the other LCOs are provided in their respective 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 reactivity worth of the regulating CEA and shutdown CEA. The SDM requirements of LCO 3.1.1, the Shutdown CEA Insertion Limits of LCO 3.1.6, the Regulating CEA Insertion Limits of LCO 3.1.7, Trip Functions 2, 14 and 15 in Table 3.3.1-1 of LCO 3.3.1, and Trip Function 1 in Table 3.3.2-1 of LCO 3.3.2 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.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.1.10.1

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

SR 3.1.10.2

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 24-hour FREQUENCY ensures that the CEAs are OPERABLE prior to reducing SDM to less than the limits of LCO 3.1.1.

SR 3.1.10.3

Verification of the reactor subcritical by more than the reactivity equivalent of the highest worth withdrawn CEA in MODE 3 is necessary to ensure that the minimum negative reactivity requirements are preserved. The minimum negative reactivity requirements are certified through the reactivity balance calculation of the following reactivity related effects:

a. Boron concentration of RCS

b. Positions of CEAs

c. Average temperature of RCS

d. Fuel burnup based on total amount of thermal energy production

e. Xenon concentration

f. Samarium concentration

Considering the slow change rate of boron concentration, the 2-hour frequency is sufficient for the operator to collect the necessary data.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.1.10.4

Within 12 hours prior to initiation of reactor startup or PHYSICS TESTS, CHANNEL FUNCTIONAL TESTS on each logarithmic and variable overpower neutron flux monitoring channel shall be performed to verify OPERABILITY of the entire channels and to adjust the setpoints with appropriate values. This ensures the Reactor Protection System is properly arranged in order to provide necessary core protection required during reactor startup or PHYSICS TESTS. During reactor startup or PHYSICS TESTS, the 12-hour FREQUENCY is sufficient time to ensure that the components supporting the plant protection and monitoring systems are OPERABLE prior to testing.

REFERENCES

1. 10 CFR 50, Appendix B, Section XI.
2. 10 CFR 50.59.
3. NRC RG 1.68, Revision 2, August 1978.
4. ANSI/ANS-19.6.1-1997.
5. DCD Tier 2, Chapter 14.
6. 10 CFR 50.46.
7. DCD Tier 2, Subsection 15.3.1.

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.11 Special Test Exceptions (STE) – MODES 1 and 2

BASES

BACKGROUND

The primary purpose of these MODES 1 and 2 STEs 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.

10 CFR 50, Appendix B, Section XI (Reference 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" (Reference 2).

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

a. Ensure facility has been adequately designed.

b. Validate analytical models used in design and analysis.

c. Verify assumptions used for predicting plant response.

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

e. Verify 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 the initial core and 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 (Reference 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.

BASES

BACKGROUND (continued)

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 as long as 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 4 defines requirements for initial testing of the facility, including PHYSICS TESTS. Requirements for reload fuel cycle PHYSICS TESTS are defined in ANSI/ANS-19.6.1-1997 (Reference 5). Although these PHYSICS TESTS are generally accomplished within the limits of all LCOs, conditions could 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) and the departure from nucleate boiling ratio (DNBR) remain within their limits, fuel design criteria are preserved.

In this test, the following LCOs are suspended:

a. LCO 3.1.4, “Moderator Temperature Coefficient (MTC)”

b. LCO 3.1.5, “Control Element Assembly (CEA) Alignment”

c. LCO 3.1.6, “Shutdown Control Element Assembly (CEA) Insertion Limits”

d. LCO 3.1.7, “Regulating Control Element Assembly (CEA) Insertion Limits”

e. LCO 3.1.8, “Part Strength Control Element Assembly (CEA) Insertion Limits”

f. LCO 3.2.2, “Planar Radial Peaking Factors (Fxy)”

g. LCO 3.2.3, “AZIMUTHAL POWER TILT (T_q)”

h. LCO 3.2.5, “AXIAL SHAPE INDEX (ASI)”

BASES

APPLICABLE SAFETY ANALYSES (continued)

The safety analysis (Reference 6) places limits on allowable THERMAL POWER during PHYSICS TESTS and requires that the LHR and the DNBR be maintained within limits. The power plateau of less than 85 % RTP and the associated trip setpoints are required to ensure that LHR and DNBR are maintained within acceptable limits.

The individual LCOs governing CEA 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 DNBR limits. The initial condition criteria for accidents sensitive to core power distribution are preserved by the LHR and DNBR limits. The criteria for the loss of coolant accident (LOCA) are specified in 10 CFR 50.46 (Reference 7). The criteria for the loss of forced reactor coolant flow accident are specified in Reference 8. Operation within the LHR limits preserves the LOCA criteria; operation within the DNBR limits preserves the loss of flow criteria. During PHYSICS TESTS, one or more of the LCOs that normally preserve the LHR and DNBR limits may be suspended. The results of the accident analysis are not adversely impacted, however, if LHR and DNBR are verified to be within their limits while the LCOs are suspended. Therefore, SRs are placed as necessary to ensure that LHR and DNBR 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 in their respective LCOs.

As described in LCO 3.0.7, compliance with Special Test Exception (STE) LCOs is optional, and therefore no SELECTION CRITERIA apply. STE LCOs provide flexibility to perform certain operations by appropriately modifying requirements of other LCOs.

A discussion of the SELECTION CRITERIA satisfied for the other LCOs are 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 non-normal CEA configurations.

d. Measure rod shadowing factors.

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 LCOs 3.1.4, 3.1.5, 3.1.6, 3.1.7, 3.1.8, 3.2.2, 3.2.3, and 3.2.5 can 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 less than 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

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 3.1.5, 3.1.6, and 3.1.7. During suspending PHYSICS TEST STE, the corresponding LCOs shall be restored.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.1.11.1

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 DNBR 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. NRC RG 1.68, Revision 2, August 1978.
4. DCD Tier 2, Chapter 14.
5. ANSI/ANS-19.6.1-1997.
6. DCD Tier 2, Chapter 15.
7. 10 CFR 50.46.
8. DCD Tier 2, Subsection 15.3.1.

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.12 Special Test Exceptions (STE) – Reactivity Coefficient Testing

BASES

BACKGROUND

The primary purpose of STEs during Reactivity Coefficient Testing is to permit relaxation of existing LCOs to allow the performance of certain PHYSICS TESTS. These tests are conducted to determine isothermal temperature coefficient, moderator temperature coefficient, and power coefficient.

10 CFR 50, Appendix B, Section XI (Reference 1) requires that a test program be established to ensure that structures, systems, and components (SSCs) 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" (Reference 2).

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

a. Ensure facility has been adequately designed.

b. Validate analytical models used in design and analysis.

c. Verify assumptions used for predicting plant response.

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

e. Verify 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 the initial core and 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 (Reference 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.

BASES

BACKGROUND (continued)

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 as long as 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-19.6.1-1997 (Reference 4). Although these PHYSICS TESTS are generally accomplished within the limits of all LCOs, conditions could 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) and the departure from nucleate boiling ratio (DNBR) remain within their limits, fuel design criteria are preserved.

In this test, the following LCOs are suspended:

a. LCO 3.1.7, “Regulating Control Element Assembly (CEA) Insertion Limits”

b. LCO 3.1.8, “Part Strength Control Element Assembly (CEA) Insertion Limits”

c. LCO 3.4.1, “RCS Pressure, Temperature, and Flow Limits” (LCO 3.4.1.b. RCS Cold Leg Temperature only)

The safety analysis (Reference 6) requires that the LHR and the DNBR be maintained within limits. The associated trip setpoints are required to ensure these limits are maintained.

BASES

APPLICABLE SAFETY ANALYSES (continued)

The individual LCOs governing CEA group height, insertion and alignment, ASI, total planar radial peaking factor, total integrated radial peaking factor, and Tq, preserve the LHR limits. Additionally, the LCOs governing Reactor Coolant System (RCS) flow, reactor inlet temperature (Tc), and pressurizer pressure contribute to maintaining DNBR limits. The initial condition criteria for accidents sensitive to core power distribution are preserved by the LHR and DNBR limits. The criteria for the loss of coolant accident (LOCA) are specified in 10 CFR 50.46 (Reference 7). The criteria for the loss of forced reactor coolant flow accident are specified in Reference 8. Operation within the LHR limit preserves the LOCA criteria. Operation within the DNBR limits preserves the loss of flow criteria.

During PHYSICS TESTS, one or more of the LCOs that normally preserve the LHR and DNBR limits may be suspended. The results of the accident analysis are not adversely impacted, however, if LHR and DNBR are verified to be within their limits while the LCOs are suspended. Therefore, SRs are placed as necessary to ensure that LHR and DNBR 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 in their respective LCOs.

As described in LCO 3.0.7, compliance with Special Test Exception (STE) LCOs is optional, and therefore no SELECTION CRITERIA apply. STE LCOs provide flexibility to perform certain operations by appropriately modifying requirements of other LCOs. A discussion of the SELECTION CRITERIA satisfied for the other LCOs are provided in their respective Bases.

BASES

LCO	This LCO permits Part Strength CEAs and Regulating CEAs to be positioned outside of their normal group heights and insertion limits, and RCS cold leg temperature to be outside its limits during the performance of PHYSICS TESTS. These PHYSICS TESTS are required to determine the isothermal temperature coefficient (ITC), MTC, and power coefficient. The requirements of LCOs 3.1.7, 3.1.8 and 3.4.1 (for RCS cold leg temperature only) may be suspended during the performance of PHYSICS TESTS provided COLSS is in service.
APPLICABILITY	This LCO is applicable in MODE 1 with THERMAL POWER greater than 20 % RTP because the reactor must be critical at THERMAL POWER levels greater than 20 % RTP to perform the PHYSICS TESTS described in the LCO section.
ACTIONS	A.1 With the LHR or DNBR outside the limits specified in their LCOs, adequate safety margin is not assured and power must be reduced to restore LHR and DNBR to within limits. The required Completion Time of 15 minutes ensures prompt action is taken to restore LHR or DNBR to within limits. B.1 When the Required Action cannot be met or 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 conditions back to within the limits of LCOs 3.1.7, 3.1.8, and 3.4.1 (for RCS cold leg temperature only). During suspending PHYSICS TEST STE, the corresponding LCOs shall be restored.
SURVEILLANCE REQUIREMENTS	SR 3.1.12.1 With THERMAL POWER greater than or equal to 20 % RTP, LHR and DNBR can be continuously monitored using the COLSS since the COLSS is available with THERMAL POWER above 20 % RTP. If COLSS is not available, LHR and DNBR can be continuously monitored using any OPERABLE CPC channel. Continuous monitoring is required to ensure that the LHR and DNBR limits are satisfied at all times. SRs 3.2.1.1 and 3.2.4.1 provide the specific requirements for performing this SR.

BASES

REFERENCES

1. 10 CFR 50, Appendix B, Section XI.
2. 10 CFR 50.59.
3. NRC RG 1.68, Revision 2, August 1978.
4. ANSI/ANS-19.6.1-1997.
5. DCD Tier 2, Chapter 14.
6. DCD Tier 2, Chapter 15.
7. 10 CFR 50.46.
8. DCD Tier 2, Subsection 15.3.1.

B 3.2 POWER DISTRIBUTION LIMITS

B 3.2.1 Linear Heat Rate (LHR)

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 accidents 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 strength CEAs to alter the axial power distribution

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

c. Correcting off optimum conditions (e.g., a CEA drop, 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 (References 1 and 2), so that specified acceptable fuel design limits (SAFDL) 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.

BASES

BACKGROUND (continued)

The power distribution is derived from the characteristics of multiple parameters and their combinations which can result in acceptable power distribution. LCOs for departure from nucleate boiling (DNB) and LHR need to be set to operate the plant within the power distribution design limit.

Proximity to the DNB condition is expressed by the DNB 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 KCE-1 Correlation (Reference 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 SAFDLs 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 exceeding the 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 (Reference 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 1,204 °C (2,200 °F) specified in the 10 CFR 50.46 (Reference 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 (Reference 4).

c. During an ejected CEA accident, the fission energy input to the fuel must not exceed 230 cal/g (Reference 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 (Reference 7).

BASES

APPLICABLE SAFETY ANALYSES (continued)

The power density at any point in the core must be limited to maintain the fuel design criteria (References 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 (Reference 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 1,204 °C (2,200 °F) (Reference 5). Peak cladding temperatures exceeding 1,204 °C (2,200 °F) cause severe cladding failure by oxidation due to a Zirconium alloy 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 F_{xy} and ASI 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 occur from conditions outside the limits of these LCOs during normal operation. However, fuel cladding damage could result if an accident 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 1,204 °C (2,200 °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.

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 1,204 °C (2,200 °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 and LHR not within the region of acceptable operation, 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 and LHR not within the region of acceptable operation. 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.

BASES

ACTIONS (continued)

Also, a maximum allowable change in the CPC calculated LHR ensures that further degradation requires the operators to take immediate action to restore LHR to within limit or reduce reactor power to comply with the Technical Specifications (TS).

With an adverse trend, one hour is allowed for restoring LHR to within limit 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. If LHR cannot be monitored every 15 minutes, assume that there is an adverse trend.

With no adverse trend, four hours is allowed to restore the LHR to within limit 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 less than 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 applicable only 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 (W/cm) 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.

REFERENCES

1. DCD Tier 2, Chapter 15.
2. DCD Tier 2, Chapter 6.
3. APR1400-F-C-TR-12002-P, Rev. 0, "KCE-1 Critical Heat Flux Correlation for PLUS7 Thermal Design Topical Report," November 2012.
4. 10 CFR 50, Appendix A, GDC 10.
5. 10 CFR 50.46.
6. NUREG-0800, Rev. 3, March 2007.
7. 10 CFR 50, Appendix A, GDC 26.

B 3.2 POWER DISTRIBUTION LIMITS

B 3.2.2 Planar Radial Peaking Factors (F_{xy})

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 accidents 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 strength 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 (References 1 and 2), so that specified acceptable fuel design limits (SAFDLs) 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.

The power distribution is derived from the characteristics of multiple parameters and their combinations which can result in acceptable power distribution. LCOs for departure from nucleate boiling (DNB) and LHR need to be set to operate the plant within the power distribution design limit.

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 KCE-1 Correlation (Reference 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.

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 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 SAFDLs 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 exceeding the 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 (Reference 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 1,204 °C (2,200 °F) specified in the 10 CFR 50.46 (Reference 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 (Reference 4).

c. During an ejected CEA accident, the fission energy input to the fuel must not exceed 230 cal/g (Reference 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 (Reference 7).

BASES

APPLICABLE SAFETY ANALYSES (continued)

The power density at any point in the core must be limited to maintain the fuel design criteria (References 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 (Reference 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 1,204 °C (2,200 °F) (Reference 5). Peak cladding temperatures exceeding 1,204 °C (2,200 °F) cause severe cladding failure by oxidation due to a Zirconium alloy 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 F_{xy} and ASI limits specified in LCOs 3.2.2 and 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 occur from conditions outside the limits of these LCOs during normal operation. However, fuel cladding damage could result if an accident 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.

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 Section 3.2 and the COLR.

Limiting of the calculated planar radial peaking factors (F^C_{xy}) used in the COLSS and CPCs to values equal to or greater than the measured planar radial peaking factors (F^M_{xy}) ensures that the limits calculated by the COLSS and CPCs remain valid.

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.

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.1.1 and A.1.2

When the F^M_{xy} values exceed the F^C_{xy} 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^C_{xy} used in the COLSS and CPCs to values greater than or equal to F^M_{xy}. 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^M_{xy} values are less than or equal to F^C_{xy} values used in the COLSS and CPCs. It ensures that the F^C_{xy} values used remain valid throughout the fuel cycle. A Frequency of 31 effective full power days (EFPD) is acceptable because the power distribution changes only slightly with the amount of fuel burnup. Determining the F^M_{xy} values after each fuel loading when THERMAL POWER is greater than 40 % RTP, but prior to its exceeding 80 % RTP, ensures that the core is properly loaded.

REFERENCES

1. DCD Tier 2, Chapter 15.
2. DCD Tier 2, Chapter 6.
3. APR1400-F-C-TR-12002-P, Rev. 0, "KCE-1 Critical Heat Flux Correlation for PLUS7 Thermal Design Topical Report," November 2012.
4. 10 CFR 50, Appendix A, GDC 10.
5. 10 CFR 50.46.
6. NUREG-0800, Rev. 3, March 2007.
7. 10 CFR 50, Appendix A, GDC 26.

B 3.2 POWER DISTRIBUTION LIMITS

B 3.2.3 AZIMUTHAL POWER TILT (T_q)

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 accidents 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 strength CEAs to alter the axial power distribution

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

c. Correcting off optimum conditions (e.g., a CEA drop, 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 (References 1 and 2), so that specified acceptable fuel design limits (SAFDLs) 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.

The power distribution is derived from the characteristics of multiple parameters and their combinations which can result in acceptable power distribution. LCOs for departure from nucleate boiling (DNB) and LHR need to be set to operate the plant within the power distribution design limit.

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 KCE-1 Correlation (Reference 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.

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 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 SAFDLs 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 exceeding the 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 (Reference 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 1,204 °C (2,200 °F) specified in the 10 CFR 50.46 (Reference 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 (Reference 4).

c. During an ejected CEA accident, the fission energy input to the fuel must not exceed 230 cal/g (Reference 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 (Reference 7).

BASES

APPLICABLE SAFETY ANALYSES (continued)

The power density at any point in the core must be limited to maintain the fuel design criteria (References 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 (Reference 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 1,204 °C (2,200 °F) (Reference 5). Peak cladding temperatures exceeding 1,204 °C (2,200 °F) cause severe cladding failure by oxidation due to a Zirconium alloy 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 F_{xy} and ASI limits specified in Subsection 3.2.2 and 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 occur from conditions outside the limits of these LCOs during normal operation. However, fuel cladding damage could result if an accident 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.

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 Section 3.2 and the COLR.

The limitations on the T_q are provided to ensure that design operating margins are maintained. T_q greater than 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 ratios at relatively low core power levels.

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 and A.2

If the measured T_q is greater than the T_q allowance used in the CPCs but less than or equal to 0.1, non-conservative 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 Action B.5 be performed if power reduction commences prior to restoring T_q less than or equal to 0.1. This requirement ensures that corrective action is taken before unrestricted power operation resumes.

If the measured T_q is greater than 0.1, THERMAL POWER is reduced to less than or equal 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 greater than 0.1 is not expected. If it occurs, continued operation of the reactor could 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 can induce an axial xenon oscillation, which results in increased linear heat generation rates 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 less than 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 variable overpower trip (VOPT) setpoints are reduced to less than or equal to 55 % RTP to ensure that the assumptions of the accident analysis regarding power peaking are maintained. After power has been reduced to less than or equal to 50 % RTP, the rate and magnitude of changes in the core flux are greatly reduced. Therefore, 8 hours is an acceptable time period to allow for reduction of the variable overpower trip setpoints, Required Action B.2. The 8-hour Completion Time allowed to reduce the variable overpower 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 is restored to within its specified limit by correcting the out of limit condition, 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 less than or equal to 0.1 at least once per hour for 12 hours or until T_q is verified to be within its specified limit at a THERMAL POWER greater than or equal to 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 less than 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.

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.

BASES

REFERENCES

1. DCD Tier 2, Chapter 15.
2. DCD Tier 2, Chapter 6.
3. APR1400-F-C-TR-12002-P, Rev. 0, "KCE-1 Critical Heat Flux Correlation for PLUS7 Thermal Design Topical Report," November 2012.
4. 10 CFR 50, Appendix A, GDC 10.
5. 10 CFR 50.46.
6. NUREG-0800, Rev. 3, March 2007.
7. 10 CFR 50, Appendix A, GDC 26.

B 3.2 POWER DISTRIBUTION LIMITS

B 3.2.4 Departure from Nucleate Boiling Ratio (DNBR)

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 accidents 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 strength CEAs to alter the axial power distribution

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

c. Correcting off optimum conditions (e.g., a CEA drop, 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 (References 1 and 2), so that specified acceptable fuel design limits (SAFDLs) 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. The power distribution is derived from the characteristics of multiple parameters and their combinations which can result in acceptable power distribution.

LCOs for departure from nucleate boiling (DNB) and LHR need to be set to operate the plant within the power distribution design limit.

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 KCE-1 Correlation (Reference 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.

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 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 SAFDLs 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 exceeding the 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 (Reference 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 1,204 °C (2,200 °F) specified in the 10 CFR 50.46 (Reference 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 (Reference 4).

c. During an ejected CEA accident, the fission energy input to the fuel must not exceed 230 cal/g (Reference 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 (Reference 7).

BASES

APPLICABLE SAFETY ANALYSES (continued)

The power density at any point in the core must be limited to maintain the fuel design criteria (References 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 (Reference 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 1,204 °C (2,200 °F) (Reference 5). Peak cladding temperatures exceeding 1,204 °C (2,200 °F) cause severe cladding failure by oxidation due to a Zirconium alloy 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 F_{xy} and ASI limits specified in LCO 3.2.2 and 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 occur from conditions outside the limits of these LCOs during normal operation. However, fuel cladding damage could result if an accident 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.

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

BASES

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 Section 3.2 and the COLR.

With the COLSS in service and one or both of the control element assembly calculator (CEAC) 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 as shown in Figure 3.2.4-1.

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 3.2.4-2, 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 3.2.4-3, 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.

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.

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

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 might 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, the allowed completion time of 1 hour is a reasonable 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.

B.1 and 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 Chapter 15 of DCD TIER 2. 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 and DNBR outside the region of acceptable operation, 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 AOO or an accident.

BASES

ACTIONS (continued)

To remedy this, the CPC calculated values of DNBR are monitored every 15 minutes when the COLSS is out of service and DNBR outside the region of acceptable operation. 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 limit or reduce reactor power to comply with the Technical Specifications (TS). With an adverse trend, one hour is allowed for restoring DNBR to within limit if the COLSS is not restored to OPERABLE status. Implementation of this requirement ensures that potential reductions in core thermal margin are quickly detected and, if necessary, cause in a decrease in reactor power and subsequent compliance with the existing COLSS out of service TS limits. If DNBR cannot be monitored every 15 minutes, assume that there is an adverse trend.

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 period is not increased. The likelihood of induced reactor transients from an early power reduction is also decreased.

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 less than 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.

BASES

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 in Figure 3.2.4-2 or 3.2.4-3 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 applicable 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.

REFERENCES

1. DCD Tier 2, Chapter 15.
2. DCD Tier 2, Chapter 6.
3. APR1400-F-C-TR-12002-P, Rev. 0, "KCE-1 Critical Heat Flux Correlation for PLUS7 Thermal Design Topical Report," November 2012.
4. 10 CFR 50, Appendix A, GDC 10.
5. 10 CFR 50.46.
6. NUREG-0800, Rev. 3, March 2007.
7. 10 CFR 50, Appendix A, GDC 26.

B 3.2 POWER DISTRIBUTION LIMITS

B 3.2.5 Axial Shape Index (ASI)

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 accidents 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 strength CEAs to alter the axial power distribution

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

c. Correcting off optimum conditions (e.g., a CEA drop, 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 (References 1 and 2), so that specified acceptable fuel design limits (SAFDLs) 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 the axial power distribution.

The power distribution is derived from the characteristics of multiple parameters and their combinations which can result in acceptable power distribution. LCOs for departure from nucleate boiling (DNB) and LHR need to be set to operate the plant within the power distribution design limit.

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 KCE-1 Correlation (Reference 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.

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 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 SAFDLs 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 exceeding the 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 (Reference 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 1,204 °C (2,200 °F) specified in the 10 CFR 50.46 (Reference 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 (Reference 4).

c. During an ejected CEA accident, the fission energy input to the fuel must not exceed 230 cal/g (Reference 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 (Reference 7).

BASES

APPLICABLE SAFETY ANALYSES (continued)

The power density at any point in the core must be limited to maintain the fuel design criteria (References 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 (Reference 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 1,204 °C (2,200 °F) (Reference 5). Peak cladding temperatures exceeding 1,204 °C (2,200 °F) cause severe cladding failure by oxidation due to a Zirconium alloy 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 F_{xy} and ASI limits specified in Section 3.2.2 and 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 occur from conditions outside the limits of these LCOs during normal operation. However, fuel cladding damage could result if an accident 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 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 DNBR operating limits. The power distribution LCO limits are provided in Section 3.2 and 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.

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.

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

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 strength 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 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 linear heat generation rates when the xenon redistributes. Reducing THERMAL POWER to less than or equal 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.

BASES

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.

REFERENCES

1. DCD Tier 2, Chapter 15.
2. DCD Tier 2, Chapter 6.
3. APR1400-F-C-TR-12002-P, Rev. 0, "KCE-1 Critical Heat Flux Correlation for PLUS7 Thermal Design Topical Report," November 2012.
4. 10 CFR 50, Appendix A, GDC 10.
5. 10 CFR 50.46.
6. NUREG-0800, Rev. 3, March 2007.
7. 10 CFR 50, Appendix A, GDC 26.

B 3.3 INSTRUMENTATION

B 3.3.1 Reactor Protection System (RPS) Instrumentation – Operating

BASES

BACKGROUND

The RPS initiates a reactor trip to protect against violating the core specified acceptable fuel design limits (SAFDL) 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.

The LSSS for variable of the significant safety functions is required by 10 CFR 50.36 (Reference 7). The LSSS, identified and maintained in the setpoint control program (SCP) controlled by 10 CFR 50.59 in conjunction with the LCOs, establishes the threshold for protection system action to prevent exceeding acceptable limits during design basis events (DBEs).

During AOOs, which are those events expected to occur one or more times during the plant life, the acceptable limits are:

a. The departure from nucleate boiling ratio (DNBR) shall be maintained above the safety limit (SL) value to prevent departure from nucleate boiling (DNB).

b. Fuel centerline melting shall not occur.

c. The reactor coolant system (RCS) pressure SL of 193.3 kg/cm^2A (2,750 psia) shall not be exceeded.

Maintaining the parameters within the above values ensures that offsite dose will be within the 10 CFR 50, Appendix A, GDC 21 (Reference 1) and 10 CFR 50.34 (Reference 2) criteria during AOOs.

BACKGROUND (continued)

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 50.34 (Reference 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.

The reactor trip system (RTS) is a safety system which initiates reactor trips. The RTS consists of four channels of sensors, auxiliary process cabinet-safety (APC-S) cabinets, excore neutron flux monitoring system (ENFMS) cabinets, core protection calculator system (CPCS) cabinets, the reactor protection system (RPS) portion of plant protection system (PPS) cabinets, and reactor trip switchgear system (RTSS) cabinets.

The RPS function is performed through the below portions in the RTS.

a. Measurement channels – consist of the sensor and transmitter providing a process value to bistable logics.

b. Bistable logics – provide trip signal to RPS logic comparing the process value with predetermined setpoint. There are two bistable racks (including separate input and output modules, data links, one bistable processor, etc.) per channel.

c. RPS logic – provides trip signal to RTSG after performing 2/4 logic based on bistable trip status of four channels. There are two local coincidence logic racks (including separate input and output modules, data links, four local coincidence logic processors, etc.) per channel.

d. RTSG – opens trip switchgear based on trip signal from RPS logic. RTSG consists of undervoltage trip equipment and shunt trip equipment. The PPS interfaces with the undervoltage trip device of RTSS breakers. The DPS interfaces with the shunt trip device of the RTSS breakers.

This LCO addresses measurement channels and bistable trip logics and automatic operating bypass removal features for those trips with operating bypasses. The RPS logic and RTSGs are addressed in LCO 3.3.4, “Reactor Protection System (RPS) Logic and Trip Initiation.” The CEACs are addressed in LCO 3.3.3, “Control Element Assembly Calculators (CEACs).”

BACKGROUND (continued)

Measurement Channels

Measurement channels, consisting of the sensor, transmitter, and related instruments, provide a measurable signal based upon the physical characteristics of the parameter being measured. The excore nuclear instrumentation and the core protection calculator systems (CPCS), though complex, are considered components in the measurement channels of the Variable Overpower – 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 can be used as inputs to engineered safety features actuation system (ESFAS) bistables, and most provide indication in the MCR. Measurement channels used as input of RPS meet the independence requirements from control signals.

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 local coincidence logic, which in turn de-energizes the initiation logic. This causes all eight RTSGs to open, interrupting power to the CEAs, allowing them to fall into the core.

Three of the four measurement channels and bistable logics channels are necessary to meet the redundancy and testability of 10 CFR 50, Appendix A, GDC 21 (Reference 1). 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.

BACKGROUND (continued)

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 removed from service until following the next MODE 5 entry. Since no single failure will either cause or prevent a protection system actuation, this arrangement meets the requirements of IEEE Standard 603 (Reference 3).

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 pre-trip signals and trip signals for each of DNBR - Low and LPD – High, and transmit the result of calculation including DNBR margin, LPD margin, and calibrated neutron flux power level to IPS and QIAS-N. The CPC channel outputs for the DNBR – Low and LPD – High trips operate contacts in the coincidence logics in a manner identical to the other RPS trip.

Each CPC receives the following inputs:

a. Hot leg and cold leg temperatures

b. Pressurizer pressure

c. Reactor coolant pump speed

d. Excore neutron flux levels

e. Target CEA position

f. 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.

BACKGROUND (continued)

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 and bistable trip units (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 within each CPC channel compare the position of each CEA to its subgroup position. If a deviation is detected by either CEAC, an annunciator sounds and appreciate “penalty factors” are transmitted to the CPC in the affected channel. These penalty factors conservatively adjust the effective operating margins to the DNBR – Low and LPD – High trips.

Each CEA has two separate reed switch position transmitter (RSPT) assemblies mounted outside the reactor coolant pressure boundary (RCPB), designated RSPT1 and RSPT2. CEA position from the RSPTs is processed by two CEA position processors (CPPs) located in each CPC channel. The CPPs transmit CEA position to appropriate CEAC in all four CPC channels over optically isolated data links, such that CEAC1 in all channels receives the position of all CEAs based upon RSPT1, and CEAC2 receives the position of all CEAs based upon RSPT2. Thus the positions of all CEAs are independently monitored by both CEACs in each CPC channel.

BACKGROUND (continued)

The CPCs display the position of each CEA on the display of IPS to be monitored by the operator. Each CPC channel is connected to the display by means of an optically isolated data link. The operator can select the channel for display. Selecting channel A or B will display CEA position based upon RSPT1 on each CEA, whereas selecting channel C or D will display CEA position based upon RSPT2 on each CEA.

CEACs are addressed in LCO 3.3.3.

Bistable Logics

The bistable logic of Plant Protection System (PPS) cabinet receives analog inputs from measurement channels. The analog input signals are directed to analog input modules in the bistable processor rack, where the analog-digital (A/D) conversion is performed. The bistable logic algorithm determines the pre-trip and trip status. Each output status is determined comparing the digitized process value from the A/D converter with the setpoint (pre-trip and trip) from the setpoint algorithm. The status of bistable logic is provided to trip indication and remote alarm.

There are four bistable channels for each RPS parameter. The bistable channels are designated A, B, C and D per measurement channels. When a trip occurs, each bistable channel provides the trip output signal to associated local coincidence logic (LCL) channels. The trip outputs are provided to LCL channels in other channel via fiber optic link for isolation.

When two or more of the bistable trip signals monitoring same parameter are in a tripped condition, the coincidence logic (two-out-of-four logic) generates a reactor trip signal.

Some measurement channels provide contact outputs to the PPS. These are DNBR – Low and LPD – High trips generated from CPCS.

BACKGROUND (continued)

The trip setpoints used in the bistables are based on the analytical limits derived from the accident analysis of DCD TIER 2 (Reference 4). 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 (Reference 5), Allowable Values specified in SCP, in the accompanying LCO, are conservatively adjusted with respect to the analytical limits. 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 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 SCP are the LSSS.

Functional testing of the entire RPS, from bistable input through the opening of individual sets of RTSGs, can be performed either at power or shut down and is normally performed on a 31-day basis. Excore nuclear instrumentation, the CPCS, and the CEACs can be similarly tested. DCD Tier 2, Section 7.2 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 local coincidence 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.

BACKGROUND (continued)

Each LCL receives four trip signals, one from its associated bistable logic in the channel and one from each of the equivalent bistable logic located in the other three channels. The LCL also receives the trip channel bypass status signals associated with each of the above mentioned bistables. The function of the LCL is to generate a coincidence signal whenever two or more like bistables are in a tripped condition. The LCL takes into consideration the trip bypass input state when determining the coincidence logics state. Designating the protection channels as A, B, C, and D, with no trip bypass present, the LCL will produce a coincidence signal for any of the following trip inputs: AB, AC, AD, BC, BD, CD, ABC, ABD, ACD, BCD, and ABCD. These represent all possible two or more trip combinations of the four protection channels. Should a trip bypass be present, the logic will provide a coincidence signal when two or more of the three un-bypassed bistables are in a tripped condition.

On a system basis, a coincidence signal is generated in all four protection channels whenever a coincidence of two or more like bistables of the four channels are in a tripped state.

In addition to a coincidence signal, each LCL also provides bypass status outputs. The bypass status is provided to verify that a bypass has actually been entered into the logic either locally or remotely via the maintenance and test panel or the operator's module.

The inputs to the initiation logic are the LCL outputs from the appropriate LCLs. The LCL outputs are arranged in the initiation circuit to provide two-out-of-four coincidence. This configuration will avoid spurious channel initiation in the event of a single LCL processor or digital output module failure. The RPS initiation logic consists of an “OR” circuit for each undervoltage and shunt trip relay and de-energizes interposing relays. Each interposing relay opens one switchgear in RTSG in turn.

Each trip path is responsible for opening two of eight RTSGs. The PPS interfaces with the undervoltage trip device of RTSS breakers. The DPS interfaces with the shunt trip device of the RTSS breakers. The actuation of either the undervoltage or the shunt trip device interrupts power from the motor generator (MG) sets to the control element drive mechanisms (CEDMs).

BACKGROUND (continued)

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. Thus, the bistable logic 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. 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 implemented in the bistable logic, so that normal trip indication is also disabled. Trips with operating bypasses include Pressurizer Pressure – Low, Logarithmic Power Level – High, and CPC (DNBR – Low and LPD – High).

Reactor Trip Switchgear (RTSG)

The reactor trip switchgear, addressed in LCO 3.3.4, consists of eight RTSGs. 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. The RTSS consists of one set of four RTSGs (RTSS 1) and another set of four RTSGs (RTSS 2). Each RTSS channel consists of two reactor trip switchgears (RTSGs). The eight RTSGs are connected with 2-out-of-4 configuration.

BASES

BACKGROUND (continued)

Each of the two trip legs consists of two RTSGs in each RTSS in series. The two RTSGs within a trip leg are actuated by separate initiation circuits.

Each set of RTSGs is operated by either a manual reactor trip switch or an interposing relay actuated by RPS. There are four manual trip switches, arranged in two sets of two. Depressing both switches in either set will result in a reactor trip.

When a manual trip is initiated using manual switches in the MCR, the RPS trip paths and relays are bypassed and the RTSG undervoltage and shunt trip devices are actuated independent of the RPS.

Manual trip circuitry includes the switches and interconnecting wiring to both RTSGs necessary to actuate both the undervoltage and shunt trip devices, but excludes the interposing relay contacts and their interconnecting wiring to the RTSGs, which are considered part of the initiation circuit.

Functional testing of the entire RPS, from bistable logic input through the opening of individual sets of RTSGs, can be performed either at power or shut down and is normally performed on a 31-day basis. DCD Tier 2, Section 7.2 (Reference 6), 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:

a. The associated actuation will occur when the monitored parameter reaches its setpoint and specific coincidence logic is satisfied.

b. 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.

APPLICABLE SAFETY ANALYSES (continued)

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 function for which no credit is taken, termed equipment protective functions, are not needed from a safety perspective.

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 SLs are not exceeded during AOOs

Category 2: To assist the ESFAS during accidents

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 RTSGs are closed.

The specific safety analysis applicable to each protective function is identified below:

1. Variable Overpower – High

The Variable Overpower – High trip provides protection against core damage during the following events:

- Uncontrolled CEA Withdrawal from Low Power (AOO)
- Uncontrolled CEA Withdrawal at Power (AOO)
- CEA Ejection (Accident)

APPLICABLE SAFETY ANALYSES (continued)

2. Logarithmic Power Level – High

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 RTSGs closed and the CEA drive system capable of CEA withdrawal, protection is required for CEA withdrawal events originating when THERMAL POWER is less than 10^{-3} % RTP. For events originating above this power level, other trips provide adequate protection.

MODES 3, 4, and 5, with the RTSGs closed, are addressed in LCO 3.3.2, “Reactor Protection System (RPS) Instrumentation – Shutdown.”

In MODES 3, 4, or 5, with the RTSGs open or the CEAs not capable of withdrawal, the Logarithmic Power Level – High trip does not have to be OPERABLE. 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 pilot operated safety relief valve (POSRV), 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)
- Main feedwater system pipe break (accident)

APPLICABLE SAFETY ANALYSES (continued)

4. Pressurizer Pressure – Low

The Pressurizer Pressure – Low trip is provided to trip the reactor to assist the ESF system in the event of LOCAs. During a LOCA, the SLs could 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.

5. Containment Pressure – High

The Containment Pressure – High trip prevents exceeding the containment design pressure during a design basis LOCA, main steam line break (MSLB), and main feedwater line break (MFLB) accident. A SIAS, CIAS, and main steam isolation signal (MSIS) 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 MFLB accident. A 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)
- Main feedwater system pipe break (accident)

APPLICABLE SAFETY ANALYSES (continued)

10, 11. Steam Generator Level – High

The Steam Generator #1 Level – High and Steam Generator #2 Level – High trips are provided to protect the turbine from excessive moisture carryover in case of a steam generator overfill event.

12, 13. Reactor Coolant Flow – Low

The Reactor Coolant Flow, Steam Generator #1 – Low and Reactor Coolant Flow, Steam Generator #2 – Low trips provide protection function against steam line break with concurrent loss of offsite power and an RCP sheared shaft event.

The low reactor coolant flow trip signal initiates a reactor trip when the measured steam generator differential pressure across the primary side of either steam generator decreases at a rate great enough to require loss of flow protection or reaches a low preset value. The trip setpoint ensures that a reactor is tripped not to exceed power density or DNBR limit.

14. 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:

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

APPLICABLE SAFETY ANALYSES (continued)

- Uncontrolled CEA withdrawal from low power
- Uncontrolled CEA withdrawal at power
- CEA misoperation; single part-strength CEA drop

For the events listed above (except CEA misoperation; single part-strength CEA drop), DNBR – Low will trip the reactor first since DNB would occur before fuel centerline melting.

15. 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.

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 (AOO)
- Increase in feedwater flow (AOO)
- Increased main steam flow (not due to steam line rupture) without turbine trip (AOO)
- Increased main steam flow (not due to steam line rupture) with a concurrent single failure of an active component (AOO)
- Steam line break with concurrent loss of offsite AC power (AOO)
- Loss of normal AC power (AOO)

APPLICABLE SAFETY ANALYSES (continued)

- Partial loss of forced reactor coolant flow (AOO)
- Total loss of forced reactor coolant flow (AOO)
- Single reactor coolant pump (RCP) shaft seizure (accident)
- Uncontrolled CEA withdrawal from low power (AOO)
- Uncontrolled CEA withdrawal at power (AOO)
- CEA misoperation; full strength CEA drop (AOO)
- CEA misoperation; part strength CEA drop (AOO)
- Primary sample or instrument line break (accident)
- Steam generator tube rupture (accident)

Interlocks/Bypasses

The bypasses and their Allowable Values are addressed in SCP. They are not otherwise addressed as specific table entries.

The automatic operating 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. Logarithmic power level – High

b. DNBR – low and LPD – High

c. Pressurizer pressure – Low

The RPS satisfies LCO SELECTION CRITERION 3.

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. With one channel in each Function trip channel bypassed, this changes the coincidence logic into a two-out-of-three logic configuration in those Functions.

Bypassing the same parameter in more than one channel is restricted by the administrative procedure. The coincidence logic becomes 2-out-of-3 coincidence logic. All-bypass function for bypassing all parameters in the channel is interlocked in LCL algorithm to prevent simultaneous bypass of more than one channel. The all-bypass interlock is implemented based on analog circuit through hardwired cable between LCLs in all channels. The purpose of all-bypass function is to support testing and maintenance of BP whereas the trip channel bypass is used against sensor failure.

Only the Allowable Values are specified for each RPS trip Function in the SCP. The nominal setpoints are selected to ensure the setpoints measured by CHANNEL FUNCTIONAL TESTS do not exceed the Allowable Value, if the channel 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 set accounting for instrument uncertainties appropriate to the trip function from the analytical limit assumed in the safety analysis.

The Bases for the individual function requirements are as follows:

1. <u>Variable Overpower – High</u>

   This LCO requires four channels of Variable Overpower – High to be OPERABLE in MODES 1 and 2.

   The variable over power trip signal initiates a reactor trip when the indicated neutron flux power increases at a rate greater than a predetermined value or reaches a high preset value.

   The flux signal to be used is the average of three linear subchannel flux signals originating from excore neutron flux monitoring system (ENFMS).

LCO (continued)

2. Logarithmic Power Level – High

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 RTSGs are closed and the CEA drive system is capable of CEA withdrawal.

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 manually when THERMAL POWER is greater than or equal to 10^{-3} % RTP to allow the reactor to be brought to power during a reactor startup. This bypass is automatically removed when THERMAL POWER is less than 10^{-3} % RTP. Above 10^{-3} % RTP, the Variable Overpower – High and Pressurizer Pressure – High trips provide protection for reactivity transients.

The trip may be manually bypassed during PHYSICS TEST pursuant to LCO 3.1.10, “Test Exceptions – SDM.” During this testing, the Variable Overpower – 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 POSRVs, and its operation avoids the undesirable operation of these valves during normal plant operation. In the event of AOO and Accident causing overpressure, this setpoint ensures the reactor trip will take place, thereby assuring the integrity of the RCPB and preventing consequent pressure rise. The POSRVs can lift to prevent overpressurization of the RCS.

LCO (continued)

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.

The trip setpoint may be manually decreased to a minimum value (floor value) of 7.0 kg/cm^{2}A (100 psia) as pressurizer pressure is reduced during controlled plant shutdowns, provided the margin between the pressurizer pressure and the setpoint is maintained less than 28.1 kg/cm^2 (400 psi). 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 logic 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 28.1 kg/cm^{2}A (400 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 35.2 kg/cm^{2}A (500 psia). The difference between the operating bypass enable and removal features allows for bypass permissive bistable hysteresis, and allows setting the operating bypass setpoint close enough to the limit so as to avoid inadvertent actuation at the 7.0 kg/cm^{2}A (100 psia) trip setpoint minimum value (floor value).

5. Containment Pressure – High

The LCO requires four channels of Containment Pressure – High to be OPERABLE in MODES 1 and 2.

LCO (continued)

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 for the 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.

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 less 14.1 kg/cm^2 (200 psi).

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.

8, 9. Steam Generator Level – Low

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 in SCP 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 steam generator via AFAS. The reactor trip will remove the heat source (except decay heat), thereby conserving the reactor heat sink.

LCO (continued)

10, 11. Steam Generator Level – High

This LCO requires four channels of Steam Generator #1 Level – High and Steam Generator #2 Level – High to be OPERABLE in MODES 1 and 2.

The Allowable Value in SCP is high enough to allow for normal plant operation and transients without causing a reactor trip. It is set low enough to ensure a reactor trip occurs before the level reaches the steam dryers. Having steam generator water level at the trip value is indicative of the plant not being operated in a controlled manner.

12, 13. Reactor Coolant Flow – Low

This LCO requires four channels of Reactor Coolant Flow – Low to be OPERABLE in MODES 1 and 2. The Allowable Value in SCP is set low enough to allow for the 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.

14. 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 Action required in the event of CEAC channel failures ensures that the CPCs are capable of performing their safety Function.

The CPC channel has many redundant feature designed to improve channel reliability. A minimum subset of features must be functional in order for the CPC to be capable of performing its safety related trip function. Therefore, the channel can remain OPERABLE in the presence of a subset of channel failures, while maintaining the ability to provide the LPD – High trip function.

LCO (continued)

On-line CPC channel diagnostics make use of redundant features to maintain channel OPERABILITY to the extent possible, and provide alarm and annunciation of detectable failures.

Those detectable CPC channel failure resulting in a loss of protective function and channel inoperability will result in a CPC fail indication and associated low DNBR and high LPD channel trips. Input failures resulting in a sensor out of range affecting one or more CPC process inputs will result in a CPC sensor failure indication.

Detectable failures, whether they result in a channel inoperability or not, are logged in a system event list.

a. Each CPC channel redundantly processes analog process and nuclear instrumentation inputs. Only one of the two redundant analog processing modules is required to maintain OPERABILITY.

b. CEA position is redundantly processed by two CPPs in each CPC channel, and transmitted to the appropriate CEACs in all four CPC channels over one way fiber-optically isolated data links. Only one source of CEC position is required to be OPERABLE to maintain channel OPERABILITY.

c. Each CPC channel has two redundant operator interface panels shared with other systems, a maintenance and test panel (MTP) in the I&C equipment room, an operator module (OM) in the MCR (MCR). At least one must be functional to assist personnel in performing certain surveillances. Upon failure of the OM, MTP, or both, the CPC channel will remain OPERABLE.

d. Each CPCS channel contains six processor modules. Failures of these modules are treated as follows:

   1. CPC processor module failure – this failure results in a CPC channel inoperability as addressed by this LCO.

   2. Auxiliary CPC processor module failure – this failure does not result in a CPC channel inoperability since this module does not perform any safety related functions.

LCO (continued)

3. CEAC1 processor module failure – this failure is addressed in LCO 3.3.3.

4. CEAC2 processor module failure – this failure is addressed in LCO 3.3.3.

5. CPP1 processor module failure – this failure is addressed in LCO 3.3.3.

6. CPP2 processor module failure – this failure is addressed in LCO 3.3.3.

The CPC channels may be manually bypassed below 10^{-4} % RTP 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 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 TESTS pursuant to LCO 3.1.10, the trip may be manually bypassed to make this test possible without reactor trip in condition less than or equal to 5% RTP.

15. 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.

LCO (continued)

The CPC channel has many redundant features designed to improve channel reliability. A minimum subset of features must be functional in order for the CPC to be capable of performing its safety related trip function. Therefore, the channel can remain OPERABLE in the presence of a subset of channel failures, while maintaining the ability to provide the DNBR – Low trip function. On-line CPC channel diagnostics make use of redundant features to maintain channel OPERABILITY to the extent possible, and provide alarm and annunciation of detectable failures.

Those detectable CPC channel failures resulting in a loss of protective function and channel inoperability will result in a CPC fail indication and associated low DNBR and high LPD channel trips. Input failures resulting in a sensor out of range affecting one or more CPC process inputs will result in a CPC sensor Failures indication.

Detectable failures, whether they result in a channel inoperability or not, are logged in a system event list.

a. Each CPC channel redundantly processes analog process and nuclear instrumentation inputs. Only one of the two redundant analog processing modules is required to maintain OPERABILITY.

b. CEA position is redundantly processed by two CPPs in each CPC channel, and transmitted to the appropriate CEACs in all four CPC channels over one way fiber-optically isolated data links. At least one CEAC is required to be OPERABLE to maintain channel OPERABILITY in each channel.

c. Each CPC channel has two redundant operator interface panels shared with other systems, such as a MTP in the instrumentation control equipment room, and an OM in the MCR. At least one must be functional to assist personnel in performing certain surveillances. Upon failure of the OM, MTP, or both, the CPC channel will remain OPERABLE.

LCO (continued)

d. Each CPCS channel contains six processor modules. Failures of these modules are treated as follows:

1. CPC processor module failure – this failure results in a CPC channel inoperability, as addressed by this LCO.

2. Aux CPC processor module failure – this failure does not result in a CPC channel inoperability since this module does not perform any safety related functions.

3. CPP1 processor module failure – this failure is addressed in LCO 3.3.3.

4. CPP2 processor module failure – this failure is addressed in LCO 3.3.3.

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 10^{-4} % RTP, 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 lower power with Pressurizer Pressure – Low or RCPs off.

During TESTS pursuant to LCO 3.1.10, the trip may be manually bypassed to make this test possible without reactor trip in condition less than or equal to 5% RTP.

BASES

LCO (continued)

Interlocks/Bypasses

The LCO on operating bypass permissive removal channels requires that the automatic operating 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 operating bypass removal channels must be OPERABLE to ensure that none of the four RPS channels are inadvertently bypassed.

This LCO applies to the operating 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.

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. Exception to this are:

The Logarithmic Power Level – High trip, RPS Logic RTSGs, and manual trip are required in MODES 3, 4, and 5, with the RTSGs 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.

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 in SCP, the channel is declared inoperable immediately and the appropriate Conditions must be entered immediately.

In the event a channel's trip setpoint is found non-conservative 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.

Two Notes have been added to the ACTIONS. Note 1 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. Note 2 has been added to ensure the function of administrative controls.

When a process measurement channel affecting redundant function equipment is inoperable, the below trip functions are placed in bypass state or trip state.

ACTIONS (continued)

Process Measurement Functions Channel		Bypass/Trip of	Trip
1.	Linear Power (Subchannel or Linear)	VOPT	(RPS)
		High LPD	(RPS)
		Low DNBR	(RPS)
2.	Pressurizer Pressure (Narrow Range)	Pressurizer High Pressure High	(RPS)
		High LPD	(RPS)
		Low DNBR	(RPS)
3.	Steam Generator Low Pressure	Steam Generator Low Pressure	(RPS)
		Steam Generator #1 Low Pressure	(ESF)
		Steam Generator #2 Low Pressure	(ESF)
4.	Steam Generator Low Level (Wide Range)	Steam Generator Low Level	(RPS)
		Steam Generator #1 Low Level	(ESF)
		Steam Generator #2 Low Level	(ESF)
5.	CPCS	High LPD	(RPS)
		Low DNBR	(RPS)

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.

ACTIONS (continued)

If one trip channel is inoperable, startup or power operation is allowed to continue, providing the inoperable channel is placed in bypass or trip in 1 hour. The 1 hour allotted to bypass or trip the trip channel is sufficient to allow the operator to take all appropriate actions for the failed trip channel and still ensures that the risk involved in operating with the failed trip channel is acceptable. The failed trip channel must be restored to OPERABLE status prior to next entry into MODE 2 following entry into MODE 5. With a trip channel in bypass, the coincidence logic is now in a two-out-of-three configuration.

The Completion Time prior to next entry into MODE 2 following entry into MODE 5 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.

The Required Action is modified by a Note stating that LCO 3.0.4 is not applicable. The Note is added to allow the changing of MODES, even though two trip channels are inoperable, with one trip channel bypassed and one tripped. In this configuration, the protection system is in a one-out-of-two logic, which is adequate to ensure that no random failure will prevent protection system operation.

Required Action B.1 provides for placing one inoperable trip channel in bypass and the other trip 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 trip channels while ensuring the risk involved in operating with the failed channels is acceptable. With one trip channel of protective instrumentation bypassed, the RPS is in a two-out-of-three logic; but with another trip channel failed, the RPS could 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 trip channel is placed in trip. This places the RPS in a one-out-of-two logic. If any of the other OPERABLE trip channels receives a trip signal, the reactor will trip.

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.

C.1, C.2.1, and C.2.2

Condition C applies to one automatic operating bypass removal Function inoperable. If the inoperable bypass removal Function for any bypass channel cannot be restored to OPERABLE status within 1 hour, the associated trip channel may be considered OPERABLE only if the bypass is not in effect. Otherwise the affected trip channel must be declared inoperable, as in Condition A, and the affected automatic trip channel placed in bypass or trip. The operating bypass removal Function and the automatic trip channel must be repaired prior to next entry into MODE 2 following entry into MODE 5. The Bases for the Required Actions and required Completion Times are consistent with Condition A.

D.1 and D.2

Condition D applies to two inoperable automatic operating bypass removal Functions. If the operating bypass removal Functions for two operating bypasses cannot be restored to OPERABLE status within 1 hour, the associated trip channel may be considered OPERABLE only if the operating bypass is not in effect. Otherwise the affected trip channels must be declared inoperable, as in Condition B, and the operating bypasses 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)

The Required Action is modified by a Note stating that LCO 3.0.4 is not applicable. The Note was added to allow the changing of MODES even though two channels are inoperable, with one channel bypassed and one tripped. In this configuration, the protection system is in a one-out-of-two logic, which is adequate to ensure that no random failure will prevent protection system operation.

E.1

Condition E is entered when the Required Action and associated Completion Time of Condition A, B, C or D 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 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 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.

The OPERABILITY of interface and test processor (ITP) is not limited per LCO 3.3.1 because ITP does not perform the safety function of RPS. However, ITP shall maintain the functional integrity to perform CHANNEL FUNCTIONAL TEST of SRs 3.3.1.7, 3.3.1.10, and 3.3.1.12.

SURVEILLANCE REQUIREMENTS (continued)

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 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. CHANNEL CHECK will detect gross channel failure; thus, it is a 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 match criteria, it could 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 protection function due to failure of redundant channels. The CHANNEL CHECK checks of channel OPERABILITY during normal operational use of the displays associated with the LCO required channels.

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 to be less than or equal to the actual RCS total flow rate measured by RCS pump differential pressure or the THERMAL POWER calculation every 12 hours when THERMAL POWER is greater than or equal to 80% RTP. The check Frequency is modified by a Note indicating “Not required to be performed until 12 hours after THERMAL POWER greater than or equal to 80% RTP”. The 12 hours after reaching 80% RTP is for plant stabilization, data taking, and flow verification.

SURVEILLANCE REQUIREMENTS (continued)

This check (if necessary, the flow measurement error by the CPC addressable constant flow coefficients adjustment and measurement method to be included in CPC BERR1 item) 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 System Event Log is checked every 12 hours to monitor the CPCS channel performance. The system event log provides a historical record of the last thirty detected CPC channel error condition including error conditions affecting the CEAC performance. A detected error condition may not render a channel inoperable, unless it is accompanied by a CPC Fail indication.

The frequency of 12 hours is based upon the nature of the surveillance in detecting many non-critical error conditions and considers that detectable failures resulting in a channel inoperability will result in a CPC Fail condition.

SR 3.3.1.4

A daily heat balance calibration is performed when THERMAL POWER is greater than or equal to 15%. The linear power level signal and the CPC addressable constant multipliers are adjusted to make the CPC ΔT power and CPC nuclear power calculations agree with the calorimetric calculation if the absolute difference is greater than or equal to 0.5%. The value of 0.5% 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 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 greater than 15% RTP to obtain accurate data. At lower power levels, the accuracy of calorimetric data is questionable.

SURVEILLANCE REQUIREMENTS (continued)

The Frequency of 24 hours is based on plant operating experience and takes into account indications and alarms located in the MCR to detect deviations in channel outputs. The Frequency is modified by Note 1 indicating this Surveillance need only be performed within 12 hours after reaching 15% RTP. The 12 hours after reaching 15% 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 greater than or equal to 80% 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 axial power distribution (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 3.3.1.11, which adjusts the gains of the three detector amplifiers for shape annealing. SR 3.3.1.6 ensures that the pre-assigned gains are still proper. Power must be greater than or equal to 15% RTP because the CPCs do not use the excore generated signals for axial flux shape information at low power levels.

SURVEILLANCE REQUIREMENTS (continued)

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.

SR 3.3.1.7

A CHANNEL FUNCTIONAL TEST on each channel is performed every 31 days to ensure the entire channels will perform its intended function when needed. The SR is modified by a Note. The Note allows the CHANNEL FUNCTIONAL TEST for the Logarithmic Power Level – High channels to be performed 2 hours after logarithmic power drops below 10^{-3} % and is required to be performed only RTSGs are closed.

The RPS CHANNEL FUNCTIONAL TEST consists of overlapping tests as described in DCD TIER 2, Section 7.2 (Reference 6). These tests verify that the RPS is capable of performing its intended function from bistable input through the RTSGs. They include:

Bistable Logic Tests

Bistable logic tests are performed to confirm that bistable logics are properly operating.

Local Coincidence Logic Tests

Local coincidence logic tests are described in LCO 3.3.4. Local coincidence logic tests are performed to confirm the operability of two-out-of-four logic and trip channel bypass logic.

Trip Path Tests

Trip path (initiation logic) tests are described in LCO 3.3.4. Initiation logic tests composed of selective two-out-of-four are performed after local coincidence logic tests are completed. These tests are performed only for one channel and one initiation logic.

SURVEILLANCE REQUIREMENTS (continued)

The RTSG test is a manually initiated test. The test is manually initiated because the test philosophy requires operator involvement in the testing and reclosing of these important reactor trip devices. The operator can obtain status information from the breaker open/close indication and current monitors and thus determine the success or failure of the test. The RTSGs must then be closed prior to testing the other three initiation circuits or a reactor trip could result.

The CPC and CEAC channels and excore nuclear instrumentation channels are tested separately.

The excore channels use pre-assigned 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 linear range excore test signal is inserted at the drawer input, since there is no preamplifier.

The CPC CHANNEL FUNCTIONAL TEST is performed every 31 days to check system operation status using MTP. The CPCS CHANNEL FUNCTIONAL TEST including trip function is performed every 18 months according to SR 3.3.1.10. The note is added to check each operable CPC have exact addressable constants in the CPCS CHANNEL FUNCTIONAL TEST.

SR 3.3.1.8

A Note indicates that excore neutron detectors are excluded from CHANNEL CALIBRATION. A CHANNEL CALIBRATION of the linear power of excore neutron flux channel every 31 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 drifts between successive calibrations to ensure that the channel remains operational between successive tests. CHANNEL CALIBRATION must be performed consistent with the SCP.

SURVEILLANCE REQUIREMENTS (continued)

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 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 MCR indications are monitored by the operators.

SR 3.3.1.9

SR 3.3.1.9 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 drifts between successive calibrations to ensure that the channel remains operational between successive tests. CHANNEL CALIBRATION must be performed consistent with the plant protection system 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 as well as operating experience and consistency with the 18-month fuel cycle.

The Surveillance is modified by a Note to indicate that the excore neutron excore 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 MCR indications are monitored by the operators.

SR 3.3.1.10

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.

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.

SR 3.3.1.11

The three excore neutron 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 the shape annealing matrix elements for the excore neutron 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 less than 80% to perform an accurate axial shape calculation used to derive the shape annealing matrix elements.

By restricting power to less than or equal to 80% 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 3.3.1.12

SR 3.3.1.12 is a CHANNEL FUNCTIONAL TEST similar to SR 3.3.1.7 is applicable only to automatic operating bypass functions and is performed once within 31 days prior to each startup. Proper operation by operating bypass permissive is critical during plant startup because the operating bypass must be in place to allow startup operation and must be automatically 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.

SURVEILLANCE REQUIREMENTS (continued)

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. Therefore, further testing of the bypass removal function after startup is unnecessary.

SR 3.3.1.13

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 RTSGs 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 × 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 or instrumentation components causing serious response time degradation, but not channel failure at power, 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.

A Note is added to indicate that the excore neutron detectors may be 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).

BASES

REFERENCES

1. 10 CFR 50, Appendix A, GDC 21.
2. 10 CFR 50.34.
3. IEEE Standard 603-1991.
4. DCD Tier 2, Chapters 6, 15.
5. 10 CFR 50.49.
6. DCD Tier 2, Chapter 7.
7. 10 CFR 50.36.

B 3.3 INSTRUMENTATION

B 3.3.2 Reactor Protection System (RPS) Instrumentation – Shutdown

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 protection 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:

a. The departure from nucleate boiling ratio shall be maintained above the safety limit (SL) value to prevent departure from nucleate boiling.

b. Fuel centerline melting shall not occur.

c. 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, Appendix A (Reference 1) and 10 CFR 50.34 (Reference 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 50.34 (Reference 2) limits.

BACKGROUND (continued)

The reactor trip system (RTS) is a safety system which initiates reactor trips. The RTS consists of four channels of sensors, auxiliary process cabinet-safety (APC-S) cabinets, excore neutron flux monitoring system (ENFMS) cabinets, core protection calculator system (CPCS) cabinets, the reactor protection system (RPS) portion of plant protection system (PPS) cabinets, and reactor trip switchgear system (RTSS) cabinets as shown in Figure 7.2-1.

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 function is performed through the below portions in the RTS.

a. Measurement channels

b. Bistable logics

c. RPS logic

d. Reactor trip switchgears (RTSGs)

This LCO applies only to the Logarithmic Power Level – High trip in MODES 3, 4, and 5 with the RTSGs closed. In MODES 1 and 2, this trip Function is addressed in LCO 3.3.1, “Reactor Protection System (RPS) Instrumentation – Operating.” LCO 3.3.13, “Logarithmic Power Monitoring Channels,” applies when the RTSGs 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 Logic

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 RTSGs, can be performed either at power or shut down and is normally performed on a 31-day basis. Nuclear instrumentation can be similarly tested. DCD Tier 2, Section 7.2 (Reference 3), provides more detail on RPS testing.

BASES

APPLICABLE SAFETY ANALYSES

The RPS functions to maintain the SLs during AOOs and mitigates the consequence of DBAs in all MODES in which the RTSGs are closed. Each of the analyzed transients and accidents can be detected by one or more RPS Functions. The Logarithmic Power Level - High trip protects the integrity ofthe 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 RTSGs 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 less than 10^{-3} %. 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 RTSGs 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 bypasses and their Allowable Values are addressed in SCP. The automatic operating 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 operating bypass for Logarithmic Power Level – High is described in Table 3.3.2-1.

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 inoperable and reduces the reliability of the affected Function.

LCO (continued)

Bypassing the same parameter in more than one channel is restricted by the administrative procedure. The coincidence logic becomes 2-out-of-3 coincidence logic. All-bypass function for bypassing all parameters in the channel is interlocked in LCL algorithm to prevent simultaneous bypass of more than one channel. The all-bypass interlock is implemented based on analog circuit through hardwired cable between LCLs in all channels. The purpose of all-bypass function is to support testing and maintenance of BP whereas the trip channel bypass is used against sensor failure. 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 RTSGs are closed and the CEA drive system is capable of CEA withdrawal.

The Allowable Value specified in the Setpoint Control Program (SCP) 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 10^{-3} % to allow the reactor to be brought to power during a reactor startup. This bypass is automatically removed when logarithmic power decreases below 10^{-3} %. Above 10^{-3} %, 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 3.1.10, “Special Test Exception (STE) – Shutdown Margin (SDM).” 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:

a. The Logarithmic Power Level – High trip, RPS Logic RTSGs, and Manual Trip are required in MODES 3, 4, and 5, with the RTSGs 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 Protection System (RPS) Logic and Trip Initiation.”

b. The Steam Generator #1 Pressure – Low trip, Steam Generator #2 Pressure – Low trip, RPS Logic, RTSGs and manual trip are required in MODES 3 and 4, with the RTSGs closed, to provide protection for MSLB. The Steam Generator Pressure – Low trip in shutdown MODE is described in LCO.

c. The Applicability is modified by a Note that allows the trip to be bypassed when logarithmic power is greater than or equal to 1×10^{-3} %, and the bypass is automatically removed when logarithmic power is less than 1×10^{-3} %.

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 SCP, 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.

ACTIONS

When a process measurement channel affecting redundant function equipment is inoperable, the below trip functions are placed in bypass state or trip state:

Process Measurement Channel	Bypass/Trip of Trip Functions	
Steam Generator Pressure	Steam Generator Low Pressure	(RPS)
	Steam Generator #1 Low Pressure	(ESF)
	Steam Generator #2 Low Pressure	(ESF)

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 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, the operation in MODES 3, 4, 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 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 next entry into MODE 2 following entry into MODE 5. With a channel in bypass, the coincidence logic is now in an two-out-of-three configuration.

The Completion Time of prior to next entry into MODE 2 following entry into MODE 5 is based on adequate channel to channel independence, which allows operation with two or more channels since no single failure will prevent a reactor trip.

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 protection instrumentation bypassed, the RPS is in a two-out-of-three logic; but with another channel failed, the RPS could 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 RTSGs 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.

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.

SURVEILLANCE REQUIREMENTS (continued)

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 could 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 protection 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 3.3.2.2

A CHANNEL FUNCTIONAL TEST on each channel is performed every 31 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. The RPS CHANNEL FUNCTIONAL TEST consists of three overlapping tests as described in DCD Tier 2, Section 7.2 (Reference 3). These tests verify that the RPS is capable of performing its intended function, from bistable input through the RTSGs. They include:

SURVEILLANCE REQUIREMENTS (continued)

Bistable Logic 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.

The SCP has controls which require verification that the instrument channel functions as required by verifying the as-left and as- found setting are consistent with those established by the setpoint methodology.

Local Coincidence Logic Tests

Local coincidence logic tests are addressed in LCO 3.3.4. Local coincidence logic tests are performed to confirm the operability of two-out-of-four logic and trip channel bypass logic.

Trip Path Test

Trip path (initiation logic) tests are described in LCO 3.3.4.

Initiation logic tests composed of two-out-of-four are performed after local coincidence logic tests are completed. These tests are performed only for one channel and one initiation logic.

The RTSG test is a manually initiated test. The test is manually initiated because the test philosophy requires operator involvement in the testing and reclosing of these important reactor trip devices. The operator can obtain status information from the breaker open/close indication and current monitors and thus determine the success or failure of the test. The RTSGs must then be closed prior to testing the other three initiation circuits, or a reactor trip could result.

The excore channels use pre-assigned 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.

SURVEILLANCE REQUIREMENTS (continued)

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 31 days prior to each startup. This SR is identical to SR 3.3.1.12. Only the Applicability differs.

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. 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.

SR 3.3.2.4

This SR is identical to SR 3.3.1.9. 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. The SCP has controls which require verification that the instrument channel functions as required by verifying the as-left and as-found setting are consistent with those established by the setpoint methodology. Allowable Values and nominal trip setpoints are specified for this RPS trip Function in the SCP 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.

SURVEILLANCE REQUIREMENTS (continued)

Each Allowable Value specified in the SCP is more conservative than the analytical limit assumed in the safety analysis in order to account for instrument uncertainties appropriate to the trip Function. A channel is inoperable if its actual trip setpoint is not within its required Allowable Value.

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 excore 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).

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.

BASES

REFERENCES

1. 10 CFR 50, Appendix A.

2. 10 CFR 50.34.

3. DCD Tier 2, Section 7.2.

B 3.3 INSTRUMENTATION

B 3.3.3 Control Element Assembly Calculators (CEACs)

BASES

BACKGROUND

The RPS initiates a reactor trip to protect against violating the SAFDLs and breaching the RCPB during AOOs. By tripping the reactor, the RPS also assists the Engineered Safety Features Actuation Systems (ESFAS) in mitigating accidents.

The protection and monitoring systems have been designed to ensure safe operation of the reactor. This is achieved by specifying 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 Values), in conjunction with the LCOs, establishes the thresholds for protection 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:

a. The DNBR shall be maintained above the safety limit value to prevent departure from nucleate boiling.

b. Fuel centerline melting shall not occur.

c. The reactor coolant system (RCS) pressure safety limit of 193.3 kg/cm^{2}A (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 (Reference 1) and 10 CFR 50.34 (Reference 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 50.34 (Reference 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.

BACKGROUND (continued)

The RPS function is performed through the portions below in the reactor trip system (RTS).

a. Measurement channels

b. Bistable logics

c. RPS logic

d. RTSG

This LCO addresses the CEACs. LCO 3.3.1 provides a description of this equipment in the RPS.

The CEACs are considered components in the measurement channels of the DNBR-Low and LPD-High trips. The CEACs are addressed by this LCO.

Each CPC receives CEA deviation penalty factors from both CEACs in that channel and uses the larger of the penalty 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 in each CPCS channel compare the position of each CEA to its subgroup position. If a deviation is detected by either CEAC, an alarm occurs and appropriate “penalty factors” are transmitted to the associated the CPC processor in that channel. These penalty factors conservatively adjust the effective operating margins to the DNBR – Low and LPD – High trips.

Each CEA has two separate reed switch position transmitter (RSPT) assemblies mounted outside the RCPB, designated RSPT1 and RSPT2. CEA position from the RSPTs is processed by CEA position processors (CPPs) located in each CPCS channel. The CPPs transmit CEA position to the appropriate CEAC in all four CPCS channels over optically isolated datalinks, such that CEAC1 in all channels receives the position of all CEAs based upon RSPT1, and CEAC2 receives the position of all CEAs based upon RSPT2. Thus, the position of all CEAs is independently monitored by both CEACs in each CPCS channel.

BACKGROUND (continued)

The CPCS displays the position of each CEA to the operator on the display of IPS. Each CPCS channel is connected to the display by means of an optically isolated data link. The operator can select the channel for display. Selecting channel A or B displays CEA position based upon RSPT1 on each CEA, whereas selecting channel C or D displays CEA position based upon RSPT2 on each CEA.

Functional testing of the entire RPS function, from bistable input through the opening of individual sets of RSTGs, can be performed either at power or shutdown and is normally performed on 31days basis. Nuclear instrumentation, the CPCs, and the CEACs can be similarly tested. 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 LCO SELECTION CRITERION 3.

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 in each channel, or that appropriate conservatism is included in the CPC calculations to account for anticipated LCO CEA deviations.

CEAC1 in all four CPC channels monitors CEA position based upon RSPT1 on all CEAs. CEAC2 in all four channels monitors CEA position based upon RSPT2 on all CEAs. Each CPC uses the higher of the two deviation penalty factors transmitted by the channel CEACs. Thus only one OPERABLE CEAC is required in each channel to provide CEA deviation protection. Because a single RSPT is used to provide RSPT input to one CEAC in all four channels, this LCO requires both CEACs to be OPERABLE in each channel so that no sensor failure resulting in CEAC failure in multiple channels can prevent a required trip from occurring.

For reliability, each CPC channel contains two CPPs, which redundantly monitor the channel RSPT inputs, perform analog to digital conversion, and transmit the CEA position to the appropriate CEAC in all four CPCS channel over separate one-way fiber optically isolated data links. The receiving CEAC will automatically switch to the backup CPP and associated data link upon failure of the preferred CPP or associated data link. CPPs in CPCS channel A or B together process all RSPT1 CEA position inputs, and transmit them to CEAC1 in all four CPC channels. Similarly, CPPs in channels C or D together process all RSPT2 position inputs, and transmit them to CEAC2 in all four CPC channels.

Operation of at least one CPP and associated data links in each CPCS channel is therefore required for both CEACs in all CPCS channels to receive CEA position information. Failure of both redundant CPPs in a channel or failure of redundant RSPT power supplies in that channel will cause the associated receiving CEACs in all channels to lose CEA position input on multiple CEAs. Failure of individual RSPTs will result in a subset of CEAs being identified as failed in the associated CEAC in multiple channels.

This LCO therefore addresses both individual channel and multiple channel CEAC inoperabilities.

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 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.

Because CEACs provide the inputs to the DNBR – Low and LPD – High trips, they are required to be OPERABLE in MODES 1 and 2 for the same reasons.

ACTIONS

One Note has been added to the ACTIONS. Note has been added to clarify the application of the Completion Time rules. The Conditions of this Specification may be entered independently for each CPC channel. The Completion Times of each inoperable channel will be tracked separately, starting from the time the Condition was entered for that channel.

A.1, A.2.1, and A.2.2

Condition A applies to the failure of one CEAC in one or more CPCS channels. A CEAC failure affecting a single channel could result from failure within a CEAC processor module, whereas a CEAC failure in multiple channels could be caused by failure of redundant CPPs within a CPC channel. Thus, Required Actions address both possibilities.

A.1

Required Action A.1 provides for declaration of affected CPCS channel inoperability within 1 hour, and entry into Required Actions associated with LCO 3.3.1 for DNBR – Low and LPD – High trip functions. This Required Action treats single CEAC failure in one or more channels in a manner consistent with other RPS failures in one or more channels, and may be the preferred action if only one CPCS channel is affected. If the failure affects more than two CPCS channels, Required Actions A.2.1 and A.2.2 would be preferable.

ACTIONS (continued)

A.2.1 and A.2.2

Required Actions A.2.1 and A.2.2 accommodate a loss of CEA position monitoring capability by one CEAC in up to all four CPCS channels. There are two CEACs per CPCS channel, each providing CEA deviation input to the associated channel CPC. CEAC is able to recognize the inoperability status of CPP and CPC is able to recognize the inoperability status of CEAC. With one failed CEAC in one or more channels, the CPC in the affected channels will receive CEA deviation penalty factors from the remaining OPERABLE CEAC. The specific Required Actions are as follows.

With one CEAC inoperable in one or more channels, the second CEAC still provides penalty factor output, CEA deviation alarm and position indication for display, etc., to the affected CPC through comparison of individual CEA in subgroup. Verification every 4 hours that each CEA is within 16.8 cm (6.6 in) 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 OPERABLE CEAC. An OPERABLE CEAC will not generate penalty factors until deviations greater than 25.1cm (9.9 in) 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.2.1 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.

B.1, B.2.1, B.2.2, B.2.3, B.2.4, and B.2.5

Condition B applies if the Required Action and associated Completion Time of Condition A are not met, or if both CEACs are inoperable in one or more CPCS channels. The Required Actions associated with this Condition involve two choices.

ACTIONS (continued)

a. Required Action B.1 immediately renders the affected CPCS channels inoperable, thus requiring entry into the Required Actions associated with LCO 3.3.1.

b. Required Action B.2.1 through B.2.5 disable the DRCS, while providing increased assurance that CEA deviations are not occurring and informing all OPERABLE CPCS 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 the CPC calculations. The penalty factor for two failed CEACs is sufficiently lower than 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

Required Action B.1 provides for declaration of affected CPC channel inoperability within 1 hour, and entry into Required Actions associated with LCO 3.3.1 for the DNBR – Low and LPD – High trip function. This Required Action treats failure of both CEACs in one or more channels in a manner consistent with other RPS failures in one or more channels. Similarly, this Required Action permits immediate declaration of channel inoperability and entry in the Required Action of LCO 3.3.1 if the Required Actions and associated Completion Times of Condition A are not met. Required Action B.1 may be the preferred action if only one CPCS channel is affected. If the failure affects more than two CPCS channels, Required Action B.2.1 through B.2.5 would be preferable.

B.2.1

Meeting the margin requirements of DNBR in LCO 3.2.4 ensures that power level is within a conservative region of operation based on actual core conditions. In addition to the above actions, RPCS must be disabled. This ensures that CEA positions will not be affected by RPCS operation.

ACTIONS (continued)

B.2.2

The upper electrical limit (UEL) CEA reed switches provide an acceptable indication of CEA position. The CEA must be maintained fully withdrawn, except as required for specified testing or flux control via group #5. This ensures that undesired perturbations in local fuel burnup are prevented.

B.2.3

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.

B.2.4

The DRCS is placed and maintained in “STANDBY,” except during CEA motion permitted by Required Action B.2.2, to prevent inadvertent motion and possible misalignment of the CEAs.

B.2.5

A comprehensive set of comparison checks on individual CEAs within groups must be made within 4 hours. Verification that each CEA is within 16.8 cm (6.6 in) 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 is entered when the Required Action and Completion Time in relation to Condition B are not met.

If the Required Actions associated with this Condition cannot be completed within the required Completion Times, the reactor must be brought to a MODE where the Required Actions are not applied. The Completion Time of 6 hours is reasonable, based on operating experience, for reaching the required MODE from full power conditions in an orderly manner without challenging plant systems.

SURVEILLANCE REQUIREMENTS

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 indicate 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 a 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 could be an indication that the sensor or the signal processing equipment has drifted outside its limits. If a channel is within the criteria, it means that the channel is 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, the CHANNEL CHECK minimizes the chance of loss of protection function due to failure of redundant channels. Channel OPERABILITY is verified by using channel related indication value requested in LCO through CHANNEL CHECK during normal operation period.

SR 3.3.3.2

The CPC System Event Log is checked every 12 hours to monitor the CPCS channel performance. The System Event Log provides a historical record of the last thirty detected CPC channel error condition including error conditions affecting the CEAC performance. A detected error condition may not render a channel inoperable, unless it is accompanied by a CPC Fail indication.

The frequency of 12 hours is based upon the nature of the surveillance in detecting many non-critical error conditions, and considers that detectable failures resulting in channel inoperability will result in a CPC Fail condition.

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.3.3

A CHANNEL FUNCTIONAL TEST on each CEAC channel is performed every 31 days to ensure the entire channel will perform its intended function when needed. The CHANNEL FUNCTIONAL TEST is performed by using MTP.

SR 3.3.3.4

CHANNEL CALIBRATION is performed every 18 months according to SR 3.3.3.4. 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 surveillance. CHANNEL CALIBRATION must be performed consistent with the CPCS specific setpoint analysis.

The decision of equipment drift size in setpoint analysis is calculated by using an 18-month calibration cycle based on operation experience and 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 practical to verify OPERABILITY, including alarm and trip Functions.

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.

REFERENCES

1. 10 CFR 50.

2. 10 CFR 50.34.

B 3.3 INSTRUMENTATION

B 3.3.4 Reactor Protection System (RPS) Logic and Trip Initiation

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.

The LSSS, defined in this Specification as the Allowable Value, in conjunction with the LCOs, establishes the threshold for protection system action to prevent exceeding acceptable limits during design basis events (DBEs).

During AOOs, which are those events expected to occur one or more times during the plant life, the acceptable limits are:

a. The departure from nucleate boiling ratio (DNBR) shall be maintained above the safety limit (SL) value to prevent departure from nucleate boiling (DNB).

b. Fuel centerline melting shall not occur.

c. The reactor coolant system (RCS) pressure SL of 193.3 kg/cm^2A (2,750 psia) shall not be exceeded.

Maintaining the parameters within the above values ensures that the offsite dose will be within the 10 CFR 50, Appendix A (Reference 1) and 10 CFR 50.34 (Reference 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 50.34 (Reference 2) limits.

BACKGROUND (continued)

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 reactor trip system (RTS) is a safety system which initiates reactor trips. The RTS consists of four channels of sensors, auxiliary process cabinet-safety (APC-S) cabinets, excore neutron flux monitoring system (ENFMS) cabinets, core protection calculator system (CPCS) cabinets, the reactor protection system (RPS) portion of plant protection system (PPS) cabinets, and reactor trip switchgear system (RTSS) cabinets.

The RPS function is performed through the below portions in the RTS.

a. Measurement channels

b. Bistable logics

c. RPS logic

d. RTSG

This LCO addresses the RPS logic and RTSGs, including manual trip capability. Measurement channels and bistable logics are described in LCO 3.3.1, “Reactor Protection System (RPS) Instrumentation – Operating.” LCO 3.3.1 provides a description of the role of this equipment in the RPS. This is summarized below:

<u>RPS Logic</u>

The RPS logic consists of both local coincidence and initiation logic includes watchdog timer monitoring the heartbeat signal of LCL processor located in initiation circuit. The RPS 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.

Each LCL receives four trip signals, one from its associated bistable logic in the channel and one from each of the equivalent bistable logic located in the other three channels. The LCL also receives the trip channel bypass status associated with each of the above mentioned bistables. The function of the LCL is to generate a coincidence signal whenever two or more like bistables are in a tripped condition.

BACKGROUND (continued)

The LCL takes into consideration the trip bypass input state when determining the coincidence logics state. Designating the protection channels as A, B, C, D, with no trip bypass present, the LCL will produce a coincidence signal for any of the following trip inputs: AB, AC, AD, BC, BD, CD, ABC, ABD, ACD, BCD, ABCD. These represent all possible two- or more out-of-four trip combinations of the four protection channels. Should a trip bypass be present, the logic will provide a coincidence signal when two or more of the three un-bypassed bistables are in a tripped condition.

On a system basis, a coincidence signal is generated in all four protection channels whenever a coincidence of two or more like bistables of the four channels are in a tripped state.

In addition to a coincidence signal, each LCL also provides bypass status outputs. The bypass status is provided to verify that a bypass has actually been entered into the logic either locally or remotely via the maintenance and test panel or the operator's module.

The inputs to the initiation logic are the LCL outputs from the appropriate LCLs. The LCL outputs are arranged in the initiation circuit to provide selective two-out-of-four coincidence. This configuration will avoid spurious channel initiation in the event of a single LCL processor or digital output module failure.

The RPS initiation logic consists of an "OR" circuit for each undervoltage and de-energizes interposing relays. Each interposing relay opens one switchgear in RTSG in turn.

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.

Thus, the bistable logic 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. Bypassing the same parameter in more than one channel is restricted by the administrative procedure. The coincidence logic becomes 2-out-of-3 coincidence logic. All-bypass function for bypassing all parameters in the channel is interlocked in LCL algorithm to prevent simultaneous bypass of more than one channel. The all-bypass interlock is implemented based on analog circuit through hardwired cable between LCLs in all channels. The purpose of all-bypass function is to support testing and maintenance of BP whereas the trip channel bypass is used for sensor failure.

BACKGROUND (continued)

RTSG

The reactor trip switchgear consists of eight RTSGs. Power input to the RTSG comes from two full capacity MG sets operated in parallel, such that the loss of either MG set does not de-energize the CEDMs. Both trip legs shall be interrupted to drop CEAs and two separate methods shall be provided because each power is connected to only one of two RTSGs connected in serial. The two RTSGs within a trip leg are actuated by separate initiation circuits. When two CEDM power supply buses are lost, all CEAs will fall into the core by gravity. The PPS interfaces with the undervoltage trip device of RTSS breakers. The DPS interfaces with the shunt trip device of the RTSS breakers. The actuation of either the undervoltage or the shunt trip device interrupts power from the motor generator (MG) sets to the control element drive mechanisms (CEDMs).

Each set of RTSG is operated by either a manual reactor trip switch or an interposing relay actuated by RPS. There are four manual trip switches, arranged in two sets of two. Depressing both switches in either set will result in a reactor trip. When a manual trip is initiated using manual switches in MCR, the RPS trip paths and relays are bypassed, and the RTSG undervoltage and shunt trip devices are actuated independent of the RPS.

Manual trip circuitry includes the switches and interconnecting wiring to both RTSGs necessary to actuate both the undervoltage and shunt trip devices but excludes the interposing relay contacts and their interconnecting wiring to the RTSGs, which are considered part of the initiation circuit.

Functional testing of the entire RPS, from bistable logic input through the opening of individual sets of RTSGs, can be performed either at power or shut down and is normally performed on a 31-day basis. DCD Tier 2, Section 7.2 (Reference 3), explains RPS testing in more detail.

Reactor Protection 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

Reactor Trip Switchgears (RTSGs)

All of the transient and accident analyses that call for a reactor trip assume that the RTSGs 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.

LCO

Reactor Protection System (RPS) Logic

The LCO on the RPS logic channels ensures that each of the following requirements are met:

a. A reactor trip will be initiated when necessary.

b. The required protection system coincidence logic is maintained (minimum two-out-of-three, normal two-out-of-four).

c. Sufficient redundancy is maintained to permit a channel to be out of service for testing or maintenance.

Failures of individual bistable logics are addressed in LCO 3.3.1.

This Technical Specification (TS) addresses failures of the RPS logic not addressed in the above, such as the failure of LCL power supplies or the failure of the trip channel bypass in the bypass condition.

Loss of a single vital bus will de-energize one of the power supplies in each LCL Channel. This will result in two RTSG opening. However, the remaining six closed RTSGs will prevent a reactor trip. For the purposes of this LCO, de-energizing up to the affected channel power supplies due to a single failure is to be treated as a single channel failure, providing the affected coincidence logic operates as designed and opens the affected RTSGs.

LCO (continued)

Each LCL receives four trip signals, one from its associated bistable logic in the channel and one from each of the equivalent bistable logic located in the other three channels. On a system basis, a coincidence signal is generated in all four protection channels whenever a coincidence of two or more like bistables of the four channels are in a tripped state. The inputs to the initiation logic are the LCL outputs from the appropriate LCLs. The LCL outputs are arranged in the initiation circuit to provide selective two-out-of-four coincidence. The reactor protection system initiation logic consists of an “OR” circuit for each undervoltage relay and de-energizes interposing relays. Each interposing relay opens one switchgear in RTSG in turn.

If a coincidence logic power supply or vital instrument bus in a channel fails, two interposing relays in the affected channel are de-energized. This will result in opening the affected RTSG.

If two RTSGs in a channel have been opened in response to a single RTSG channel, initiation logic channel, or manual trip channel failure, the affected RTSG may be closed for up to 1 hour for Surveillance on the initiation logic channel, RTSG, and manual trip channels. In this case, the redundant RTSG will provide protection if a trip should be required.

1. Coincidence Logic

This LCO requires four coincidence logic channels to be OPERABLE in MODES 1 and 2, and in MODES 3, 4, and 5 when the RTSGs are closed and any CEA is capable of being withdrawn.

2. Initiation Logic

This LCO requires four initiation logic channels to be OPERABLE in MODES 1 and 2, and in MODES 3, 4, and 5 when the RTSGs are closed and any CEA is capable of being withdrawn.

LCO (continued)

3. RTSG

The LCO requires four RTSG channels to be OPERABLE in MODES 1 and 2, and in MODES 3, 4, and 5 when the RTSGs are closed and any CEA is capable of being withdrawn.

Each channel of RTSGs starts at the interposing relay contact and the manual trip contact for each breaker. Manual trip contacts and upstream circuitry are considered to be manual trip circuitry.

A Note associated with the ACTIONS states that if one RTSG has been opened in response to a single RTSG channel, initiation logic channel, or manual trip channel failure, the affected RTSG may be closed for up to 1 hour for Surveillance on the OPERABLE initiation logic, RTSG, and manual trip channels.

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 RTSGs are closed and any CEA is capable of being withdrawn.

Two independent sets of two adjacent switches are provided at separate locations. Each switch is considered a channel and operates two of the eight RTSGs. Depressing both push switches 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 switch circuit can either cause or prevent a reactor trip.

Manual trip switches are also provided at the RTSG (locally) in case the main control room (MCR) push buttons become inoperable or the MCR becomes uninhabitable. These are not part of the RPS and cannot be credited in fulfilling the LCO operability requirements. Furthermore, LCO 3.3.4 ACTIONS need not be entered due to failure of a local manual trip.

BASES

APPLICABILITY

The RPS logic channels (coincidence logic, initiation logic), RTSGs, and manual trip channels are required to be OPERABLE in MODE 1, 2 and MODES 3, 4, and 5 when the CEAs are capable of being withdrawn and RTSGs are closed. RPS instrument in MODES 1 and 2 is described in LCO 3.3.1. When the CEAs are capable of being withdrawn and RTSGs are closed, RPS instrument in MODES 3, 4, and 5 are described in LCO 3.3.2. CEAC in MODES 1 and 2 is described in LCO 3.3.3.

The RPS logic, RTSGs, and manual trip are required to be OPERABLE in any MODE when any CEA is capable of being withdrawn from the core (i.e., RTSGs 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 RTSGs 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 indicate a boron dilution event. This is addressed in LCO 3.3.14, “Boron Dilution Alarm.”

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.

A.1

Condition A applies to one coincidence logic channel, one initiation logic channel, RTSG channel, or manual trip channel in MODES 1 and 2, since they have the same ACTIONS. MODES 3, 4, and 5, with the RTSGs closed, are addressed in Condition B. These Required Actions require opening the affected RTSGs.

This removes the need for the affected channel by performing its associated safety function. With an RTSG open, the affected Functions are in 2-out-of-3 logic, which meets redundancy requirements, but testing on the OPERABLE channels cannot be performed without causing a reactor trip unless the RTSGs in the inoperable channels are closed to permit testing.

ACTIONS (continued)

Therefore, a Note has been added, specifying that the RTSGs associated with one inoperable channel may be closed for up to 1 hour for the performance of an RPS CHANNEL FUNCTIONAL TEST.

Required Action A.1 provides for opening the RTSGs associated with the inoperable channel within a Completion Time of 1 hour. This Required Action is conservative, since depressing the manual trip switch 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 RTSGs while maintaining the risk of having them closed at an acceptable level.

B.1

Condition B applies to the failure of one initiation logic channel, RTSG channel, or manual trip channel affecting the same trip leg in MODE 3, 4, or 5 with the RTSGs 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 RTSGs must be opened so the affected functions are one-out-of-two logic which meets redundancy requirements.

The Completion Time of 48 hours is adequate to repair most failures.

Testing on the OPERABLE channels cannot be performed without causing a reactor trip, unless the RTSGs in the inoperable channels are closed to permit testing. Therefore, a Note has been added specifying that the RTSGs associated with one inoperable channel may be closed for up to 1 hour for the performance of an RPS CHANNEL FUNCTIONAL TEST.

C.1

Condition C applies to the failure of both initiation logic channels affecting the same trip leg. Since this will open two channels of RTSGs, this Condition is also applicable to channels in the same trip leg. This will open both RTSGs in the affected trip leg, satisfying the Required Action of opening the affected RTSGs.

ACTIONS (continued)

Of greater concern is the failure of the initiation circuit in a non-trip condition. With only one RPS logic channel failed in a non-trip condition, there is still the redundant set of RTSGs in the trip leg.

With both failed in a non-trip condition, the reactor will not trip automatically when required. In either case, the affected RTSGs must be opened immediately by using the appropriate manual trip push switches, since each of the four push buttons opens one RTSG. Caution is required since reactor will be shut down by pushing unrelated switches.

If the affected RTSG cannot be opened, Required Action D is entered. This would only occur if there is a failure in the manual trip circuitry or the RTSGs.

D.1 and D.2

Condition D is entered if Required Actions associated with Condition A or C are not met within the required Completion Time or if for one or more functions, more than one logic (coincidence logic, initiation logic), manual trip channel, or RTSG channel is inoperable for reasons other than Condition C.

If the RTSGs associated with the inoperable channel cannot be opened, the reactor must be shut down within 6 hours and all the RTSGs 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 RTSGs. All RTSGs should then be opened, placing the plant in a MODE where the LCO does not apply and ensuring no CEA withdrawal occurs.

SURVEILLANCE REQUIREMENTS

The OPERABILITY of the ITP is not limited per LCO 3.3.4 because ITP does not perform the safety function of RPS. However, the ITP shall maintain the functional integrity to perform CHANNEL FUNCTIONAL TEST of SR 3.3.4.1 and 3.3.4.2.

SR 3.3.4.1

A CHANNEL FUNCTIONAL TEST on each channel is performed every 31 days to ensure the entire channel will perform its intended function when needed.

SURVEILLANCE REQUIREMENTS (continued)

The RPS CHANNEL FUNCTIONAL TEST consists of overlapping tests as described in DCD Tier 2, Section 7.2 (Reference 3). These tests verify that the RPS is capable of performing its intended function, from bistable input through the RTSGs.

Bistable logic test is described in SR 3.3.1.7. This SR describes two kinds of test related to RPS logic which includes coincidence logic and trip path (initiation logic).

LCL Testing

Automatic LCL testing is performed to verify the operability of two-out-of-four logic and trip channel bypass logic.

Trip Path Testing

The RTSG test is a manually initiated test. The test is manually initiated because the test philosophy requires operator involvement in the testing and reclosing of these important reactor trip devices. The operator can obtain status information from the breaker open/close indication and current monitors and thus determine the success or failure of the test. The RTSGs must then be closed prior to testing the other three initiation circuits, or a reactor trip could result.

SR 3.3.4.2

Each RTSG is actuated by an undervoltage coil and a shunt trip coil. De-energizing the undervoltage coil or energizing the shunt trip coil will cause the circuit breaker to open. The PPS interfaces with the undervoltage trip device of RTSS breakers. The DPS interfaces with the shunt trip device of the RTSS breakers. The actuation of either the undervoltage or the shunt trip device interrupts power from the motor generator (MG) sets to the control element drive mechanisms (CEDMs). When an RTSG is opened, either during an automatic reactor trip or by using the manual push switches in the MCR, the undervoltage coil is de-energized and the shunt trip coil is energized. This makes it possible 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 must remain de-energized, preventing their operation. Conversely, during shunt trip coil testing, the undervoltage coils must remain energized, preventing their operation.

BASES

SURVEILLANCE REQUIREMENTS (continued)

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 RTSG 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.

SR 3.3.4.3

A CHANNEL FUNCTIONAL TEST on the manual trip channels is performed periodically once every 31 days to ensure the entire channel will perform its intended function if required.

REFERENCES

1. 10 CFR 50, Appendix A.
2. 10 CFR 50.34.
3. DCD Tier 2, Section 7.2.

B 3.3 INSTRUMENTATION

B 3.3.5 Engineered Safety Features Actuation System (ESFAS) Instrumentation

BASES

BACKGROUND

The ESFAS initiates necessary safety systems, based upon the values of selected unit parameters, to protect against violating core design limits and 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 protection 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, 6. Auxiliary Feedwater Actuation Signal (AFAS)

The equipment actuated by each of the above signals is identified in the DCD Tier 2, Section 7.3 (Reference 1).

The engineered safety features (ESF) system consists of four channels of sensors, APC-S cabinets, the ESF signal initiation portion of the PPS cabinets and ESF-CCS.

The ESFAS function is performed through the below portions in the ESF system.

- Measurement channels
- Bistable logic
- ESFAS logic:
  - Coincidence logic
  - Initiation logic channel
  - Actuation logic

BACKGROUND (continued)

This LCO addresses measurement channels and bistable logic. Logic is addressed in LCO 3.3.6, “Engineered Safety Features Actuation System (ESFAS) Logic and Manual Trip.”

The role of each of these functions in the ESFAS, including the logic of LCO 3.3.6, is discussed below.

Measurement Channels

Measurement channels, consisting of the sensor, transmitter and signal conditioning devices 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 bistable processors within the same ESFAS channel. In addition, some measurement channels are used as inputs to reactor protection system (RPS) bistable processors and provide indication in the MCR.

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 NSSS ESFAS bistables monitoring the same parameter will generate initiation signal in local coincidence logic. This causes both channels of actuation logic to respond. Each channel of actuation logic controls one train of the associated engineered safety features (ESF) equipment.

Three of the four measurement channels and bistable processors are necessary to meet the redundancy and testability of 10 CFR 50, Appendix A, GDC 21 (Reference 2).

The fourth channel provides additional flexibility, by allowing one channel to be removed from service for maintenance or testing, while still maintaining a minimum two-out-of-three logic.

Since no single failure will prevent a protection system actuation, this arrangement meets the requirements of IEEE 603 (Reference 3).

BACKGROUND (continued)

Bistable Logics

The bistable trip unit, mounted in the plant protection system (PPS) cabinet, receives an analog input from the measurement channels. The analog signal then converted into digital in the analog input module of bistable processor. The bistable trip algorithm decides the pretrip and trip status. Each output status is derived through comparing the digitalized process values by A/D converter to the setpoints (pretrip and trip). The output status of bistable trip logic is provided to the local coincidence logic. In addition, the status is provided for trip indication and remote alarm.

There are four bistable logic channels for each ESFAS function corresponding to each measurement channel (A, B, C, and D). When two ESFAS functions share the same input and trip setpoints (e.g., containment pressure being inputted to CIAS and SIAS), bistable logic output in one channel can be used for two safety Functions. Similarly, RPS and ESFAS can share bistable logic (e.g., Pressurizer Pressure – Low inputs to RPS and SIAS). When a trip occurs, each bistable logic channel provides a trip output signal to the corresponding coincidence logic. The trip status in one channel is sent to the local coincidence logic in the other channels through fiber-optic links for isolation.

The local coincidence logic (two-out-of-four logic) generates the ESFAS initiation signal when two or more bistable logics are in tripped condition. The trip setpoints and Allowable Values used in the bistables based on the analytical limits stated in Chapter 15 (Reference 4). 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 (Reference 5), Allowable Values specified in SCP, in the accompanying LCO, are conservatively adjusted with respect to the analytical limits. 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 in SCP.

BACKGROUND (continued)

Setpoints in accordance with the Allowable Value will ensure that Safety Limits (SLs) 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 output to the ESFAS actuation logic, can be performed either at power or shut down, and is normally performed on a monthly basis (31 days). DCD Tier 2, Section 7.2 (Reference 6) 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.

ESFAS Logic

The ESFAS logic, consisting of initiation logic channel and actuation logic, employs a scheme that provides an ESF actuation of all trains when bistables in any two of the four channels sensing the same input parameter trip. This is called a two-out-of-four trip logic.

Each LCL receives four trip signals, one for its associated bistable logic in the channel and one from each of the equivalent bistable logic located in the other three channels. The LCL receives the trip channel bypass status associated with each of the above mentioned bistables. The function of the LCL is to generate a coincidence signal whenever two or more like bistables are in a tripped condition. The LCL takes into consideration the trip bypass input state when determining the coincidence logics state. Designating the protection channels as A, B, C, D, with no trip bypass present, the LCL will produce a coincidence signal for any of the following trip inputs: AB, AC, AD, BC, BD, CD, ABC, ABD, ACD, BCD, ABCD. These represent all possible two- or more out-of-four trip combinations of the four protection channels. Should a trip bypass be present, the logic will provide a coincidence signal when two or more of the three un-bypassed bistables are in a tripped condition.

BACKGROUND (continued)

On a system basis, a coincidence signal is generated in all four protection channels whenever a coincidence of two or more like bistables of the four channels are in a tripped state. The local coincidence trip output in coincidence logic is used as an input to the initiation logic. This signal is sent to actuation logic in each channel of ESF-CCS.

The actuation logic in each channel of ESF-CCS takes part in corresponding ESFAS train. Each ESF Function has individual actuation logic in each channel of ESF-CCS.

The initiation logic performs the logical “OR” of LCL outputs for each ESFAS signal and sends the ESFAS signal to ESF-CCS

The ESF-CCS comprises power supply, manual switch, latching logic and serial data link for group and loop controllers.

Each ESFAS Function has sub groups and each sub group is in charge of one- or more ESFAS Functions. The initiation and actuation logics to the sub groups are identified in LCO 3.3.6.

By trip channel bypassing one input parameter for a channel, the two-out-of-four ESFAS coincidence logic shall be converted to two-out-of-three. Though the bypass produces trip indication and alarm in the bistable processor, the LCL does not accept the corresponding input signal as an input for actuation. Different parameters may be simultaneously bypassed, either in one channel or in different channels. Bypassing the same parameter in more than one channel is restricted by the administrative procedure. The coincidence logic becomes 2-out-of-3 coincidence logic. All-bypass function for bypassing all parameters in the channel is interlocked in LCL algorithm to prevent simultaneous bypass of more than one channel. The all-bypass interlock is implemented based on analog circuit through hardwired cable between LCLs in all channels. The purpose of all-bypass function is to support testing and maintenance of BP whereas the trip channel bypass is used against sensor failure.

In addition to the trip channel bypasses, there are also operating bypasses for ESFAS actuation trip. 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.

BASES

BACKGROUND (continued)

Operating bypass protects the output of trip and alarm signals from bistable processor. The Pressurizer Pressure – Low input to the SIAS shares an operating bypass with the Pressurizer Pressure – Low reactor trip.

When necessary, the operator can manually actuate the ESFAS in the MCR and local panel.

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 can be the primary actuation signal for more than one type of accident. An ESFAS Function can also be the secondary, or backup, actuation signal for one or more other accidents.

ESFAS protection Functions are as follows:

1. Safety Injection Actuation Signal (SIAS)

   SIAS ensures acceptable consequences during large break loss of coolant accidents (LOCAs), small break LOCAs, control element assembly (CEA) ejection accidents, steam generator tube rupture, and main steam line breaks (MSLBs). To provide the required protection, either a high containment pressure or a low pressurizer pressure signal will initiate SIAS. The SIAS initiates the safety injection system (SIS) and actuates emergency diesel generator (EDG).

2. Containment Spray Actuation Signal (CSAS)

   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.

3. Containment Isolation Actuation Signal (CIAS)

   CIAS ensures acceptable mitigating actions during large and small break LOCAs, and MSLBs inside containment or FWLBs either inside or outside containment. CIAS is initiated by low pressurizer pressure or high containment pressure.

APPLICABLE SAFETY ANALYSES (continued)

4. Main Steam Isolation Signal (MSIS)

MSIS ensures acceptable consequences during an MSLB, small LOCA, or FWLB (between the steam generator and the main feedwater check valve), either inside or outside containment. MSIS isolates both steam generators if either steam generator indicates a low pressure condition, if a high containment pressure condition exists or if either steam generator indicates a high level condition.

This prevents an excessive rate of heat extraction and subsequent cooldown of the RCS during these events.

5, 6. Auxiliary Feedwater Actuation Signal (AFAS)

AFAS consists of two steam generator specific signals (AFAS-1 and AFAS-2). AFAS-1 initiates auxiliary feed to SG #1 and AFAS-2 initiates auxiliary feed to SG #2.

AFAS maintains a steam generator heat sink during steam generator tube rupture event, small LOCA, MSLB, or FWLB event either inside or outside containment.

The ESFAS satisfies LCO SELECTION CRITERION 3.

LCO

The LCO requires all channel equipment necessary for ESFAS actuation, to be OPERABLE.

The bases for the LCOs on ESFAS Functions are:

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, 3, and 4.

The Containment Pressure – High signal is shared among the SIAS (Function 1), CIAS (Function 3), and MSIS (Function 4).

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 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, 3 and 4.

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 7.0 kg/cm^{2}A (100 psia) during MODES 3 and 4 by maintaining the margin between pressurizer pressure and the trip setpoint less than or equal to 28.1 kg/cm^2 (400 psi).

The margin between actual pressurizer pressure and the trip setpoint must be maintained less than or equal to the specified value 28.1 kg/cm^2 (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.

LCO (continued)

When the trip setpoint has been lowered below the operating bypass permissive setpoint of 28.1 kg/cm^{2}A (400 psia), the Pressurizer Pressure – Low reactor trip, CIAS, and SIAS actuation may be manually bypassed in preparation for shutdown cooling. When pressurizer pressure rises above bypass removal setpoint of 35.2 kg/cm^{2}A (500 psia), the bypass is removed.

Bypass Removal

This LCO requires the operating bypass removal function for all four Pressurizer Pressure – Low trip channels to be OPERABLE in MODES 1, 2, 3, and 4.

Each of the four channels enables and disables the operating bypass capability for a single channel. Therefore, this LCO applies to the operating bypass removal feature only. If the operating bypass enable function is failed so as to prevent entering a bypass condition, operation may continue. Since the trip setpoint has a floor value of 7.0 kg/cm^{2}A (100 psia), a channel trip will result if pressure is decreased below this setpoint without bypassing.

The operating 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.

LCO (continued)

2. Containment Spray Actuation Signal

Containment spray is initiated either manually or automatically. For an automatic actuation, it is necessary to have a Containment Pressure – High High signal. 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. 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, 3 and 4.

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

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 local coincidence logic. The remainder of the initiation channels, the manual channels, and the actuation logic are separate and are addressed in LCO 3.3.6.

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).

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 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.

The Pressurizer Pressure – Low trip setpoint, which provides an SIAS, CIAS, and RPS trip, may be manually decreased to a value of 7.0 kg/cm^2A (100 psia) during MODE 3 by maintaining the margin between pressurizer pressure and the trip setpoint less than or equal to 28.1 kg/cm^2 (400 psi). The safety margin between actual pressurizer pressure and the trip setpoint must be maintained less than or equal to the specified value 28.1 kg/cm^2 (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.

LCO (continued)

When the trip setpoint has been lowered below the operating bypass removal setpoint of 28.1 kg/cm^{2}A (400 psia), the pressurizer pressure – Low reactor trip, CIAS, and SIAS actuation may be manually bypassed in preparation for shutdown cooling. When pressurizer pressure rises above bypass removal setpoint of 35.2 kg/cm^{2}A (500 psia), the bypass is removed.

Bypass Removal

This LCO requires the bypass removal Function for all four Pressurizer Pressure – Low trip channels to be OPERABLE in MODES 1, 2, and 3. Each of the four channels enables and disables the operating bypass capability for a single channel. Therefore all four operating bypass removal channels must be OPERABLE to ensure that none of the four channels are inadvertently bypassed.

This LCO applies to the operating bypass removal feature only. If the operating bypass enable Function is failed so as to prevent entering a bypass condition, operation may continue. Since the trip setpoint has a floor value of 7.0 kg/cm^{2}A (100 psia), a channel trip will result if pressure is decreased below this setpoint without bypassing.

The operating bypass removal Allowable Value was chosen because MSLB events originating from below this setpoint add less positive reactivity than that which can be compensated by required SDM.

4. Main Steam Isolation Signal

The LCO is applicable to the MSIS in MODE 1, 2, 3, and 4 except when all associated valves are closed and deactivated.

a. Steam Generator Pressure – Low

This LCO requires four channels of Steam Generator Pressure – Low to be OPERABLE in MODES 1, 2, 3 and 4.

LCO (continued)

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.

An RPS trip on Steam Generator Pressure – Low is initiated simultaneously, using the same bistable.

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 steam generator pressure and the trip setpoint must be maintained less than or equal to the specified value of 14.1 kg/cm^2 (200 psi) 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, 3 and 4. 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 not indicative of an abnormal condition. The setting is low enough to initiate the ESF Functions when an abnormal condition is indicated. When decreasing pressurizer pressure, the pressure may be manually decreased to a value of 7.0 kg/cm^{2}A (100 psia) during MODES 3 and 4 by maintaining the margin between pressurizer pressure and the trip setpoint less than or equal to 28.1 kg/cm^2 (400 psi).

LCO (continued)

c. Steam Generator Level – High

This LCO requires four channels of Steam Generator Level – High to be OPERABLE in MODES 1, 2, 3, and 4.

The Allowable Value for this trip is set high enough not to effect normal operation. The setting is low enough to protect secondary side equipment during abnormal increase of steam generator level.

5, 6. Auxiliary Feedwater Actuation Signal SG #1 and SG #2 (AFAS-1 and AFAS-2)

AFAS-1 is initiated to SG #1 by a low steam generator level. AFAS-2 is similarly configured to feed AFW into SG #2.

The following LCO description applies to both AFAS signals.

a. Steam Generator Level – Low

This LCO requires four channels of Steam Generator Level – Low to be OPERABLE for each AFAS in MODES 1, 2, and 3.

The Steam Generator Level – Low AFAS input is derived from the Steam Generator Level – Low PPS bistable output. AFAS is initiated well before steam generator inventory is challenged.

APPLICABILITY

In MODES 1, 2, 3 and 4, there is sufficient energy in the primary and secondary systems to warrant the automatic ESF system responses below. However, in MODE 4, some parts of ESFAS actuation do not require automatic response (see Table 3.3.5-1):

a. Close main steam isolation valves to preclude a positive reactivity addition.

b. Actuate auxiliary feedwater to preclude the loss of the steam generators as a heat sink (in the event the normal feedwater system is not available).

BASES

APPLICABILITY (continued)

c. 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.

d. 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 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 trip setpoint is found non-conservative 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 one channel of process measurement circuit effecting multiple functioning equipment is in test or inoperable, all the following associate functioning equipment is set to bypassed or tripped.

ACTIONS (continued)

Process Measurement Circuits	Bypass/ Trip of Functioning Equipment
1. SG Pressure – Low	
SG Pressure Low	(RPS)
SG #1 Pressure Low	(ESF)
SG #2 Pressure Low	(ESF)
2. SG Level – Low (WR)	
SG Level Low	(RPS)
SG #1 Level Low	(ESF)
SG #1 Level Low	(ESF)

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.

Two Notes have been added in the ACTIONS. Note 1 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. Note 2 is added to ensure review by the administrative control is performed to discuss the desirability of maintaining the channel in the bypassed condition.

A.1 and A.2

Condition A applies to the failure of a single channel of one or more input parameters in any ESFAS Function as following:

1. SIAS

   Containment Pressure – High
   Pressurizer Pressure – Low

2. CSAS

   Containment Pressure – High High

ACTIONS (continued)

3. CIAS

Containment Pressure – High
Pressurizer Pressure – Low

4. MSIS

Steam Generator Pressure – Low
Containment Pressure – High
Steam Generator Level – High

5. AFAS-1

Steam Generator #1 Level – Low

6. AFAS-2

Steam Generator #2 Level – 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 is restored to OPERABLE status prior to next entry into MODE 2 following entry into MODE 5. With a channel bypassed, the coincidence logic is 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 next entry into MODE 2 following entry into MODE 5 is based on adequate channel to channel independence, which allows a two-out-of-three channel operation, since no single failure will prevent a ESFAS initiation.

ACTIONS (continued)

B.1

The Required Action is modified by a Note stating that LCO 3.0.4 is not applicable. The Note was added to allow the changing of MODES even though two channels are inoperable, with one channel bypassed and one tripped. In this configuration, the protection system is in a one-out-of-two logic, which is adequate to ensure that no random failure will prevent protection system operation.

Condition B applies to the failure of two channels of one or more input parameters in any AFAS automatic trip Function as following:

1. SIAS

   Containment Pressure – High
   Pressurizer Pressure – Low

2. CSAS

   Containment Pressure – High High

3. CIAS

   Containment Pressure – High
   Pressurizer Pressure – Low

4. MSIS

   Steam Generator Pressure – Low
   Containment Pressure – High
   Steam Generator Level – High

5. AFAS-1

   Steam Generator #1 Level – Low

6. AFAS-2

   Steam Generator #2 Level – Low

ACTIONS (continued)

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 protection instrumentation bypassed, the ESFAS Function is in two-out-of-three logic in the bypassed input parameter, but with another channel failed, the ESFAS could 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.

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 operating bypass removal function inoperable. The only automatic operating 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 function for any operating bypass cannot be restored to OPERABLE, the associated ESFAS channel may be considered OPERABLE only if the operating 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 operating bypass removal channel repaired. The Bases for the Required Actions and required Completion Times are consistent with Condition A.

ACTIONS (continued)

D.1 and D.2

The Required Action is modified by a Note stating that LCO 3.0.4 is not applicable. The Note was added to allow the changing of MODES even though two channels are inoperable, with one channel bypassed and one tripped. In this configuration, the protection system is in a one-out-of-two logic, which is adequate to ensure that no random failure will prevent protection system operation.

Condition D applies to two inoperable automatic operating bypass removal functions within a completion time of 1 hour. If the bypass removal Functions for two operating bypasses cannot be restored to OPERABLE, the associated ESFAS channel may be considered OPERABLE, only if the bypass is not in effect. Otherwise the affected ESFAS channels must be declared inoperable, as in Condition B, and either the bypasses removed, or the operating bypass removal functions 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.

E.1 and E.2

If the Required Actions and associated Completion Times for SIAS, CIAS, and AFAS Functions 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 the Required Actions and associated Completion Times for CSAS and MSIS functions 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 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

Since the ITP does not perform safety related function for ESFAS, OPERABILITY per LCO 3.3.5 is not required. However, the ITP shall maintain the functional integrity for the CHANNEL FUNCTIONAL TEST in SRs 3.3.5.2, 3.3.5.3, and 3.3.5.5.

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 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. CHANNEL CHECK will detect gross channel failure; thus, it is a 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 match criteria, it could be an indication that the sensor or the signal processing equipment has drifted outside its limit. If the channels are within the match criteria, it is an indication that the channels are OPERABLE.

The CHECK FREQUENCY, twice a day, 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 protection function due to failure of redundant channels.

The CHANNEL CHECK supplements checks of channel OPERABILITY during normal operational use of displays associated with the LCO required channels.

SR 3.3.5.2

A CHANNEL FUNCTIONAL TEST on each channel is performed every 31 days to ensure the entire channel will perform its intended function when needed. This test is part of an overlapping test sequence similar to that employed in the RPS.

SURVEILLANCE REQUIREMENTS (continued)

This sequence consists of SRs 3.3.5.2, 3.3.6.1, and 3.3.6.2 and tests the entire ESFAS from bistable input to actuational output. These overlapping tests are described in DCD Tier 2 Section 7.3 (Reference 1).

SRs 3.3.5.2 and 3.3.6.1 are performed together and in conjunction with ESFAS testing. SR 3.3.6.2 verifies that each subgroup can actuate ESFAS equipment when actuational output of each subgroup is generated.

These tests verify that the ESFAS is capable of performing its intended function, from bistable through the actuated components. SRs 3.3.6.1 and 3.3.6.2 are described in LCO 3.3.6. SR 3.3.5.2 includes bistable logic testing.

To assure the trip occurrence by bistable logic within Allowable Value of setpoint, test signal is infected in only one channel at a time. This is performed in bypassed status of corresponding RPS trip channel. Setpoint adjustment must be performed consistent with the plant specific setpoint analysis.

SR 3.3.5.3

CHANNEL CALIBRATION is a complete check of the instrument channel including the detector and the operating 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 drifts between successive calibrations to ensure that the channel remains operational between successive Surveillances. CHANNEL CALIBRATION must be performed consistent with the plant specific setpoint analysis.

The 18-month Frequency is based upon the possibility for the necessity of surveillance activity and upon the unexpected transients in case when the check is performed at plant operation.

SR 3.3.5.4

This Surveillance ensures that the actuation response times are within the maximum values assumed in the safety analyses.

Response time testing acceptance criteria are included in DCD Tier 2 Section 7.3 (Reference 1).

SURVEILLANCE REQUIREMENTS (continued)

ESF RESPONSE TIME tests are conducted on a STAGGERED TEST BASIS of once every 18 months. The 18-month Frequency is based upon plant operating experience, which shows that random failures of instrumentation components causing serious response time degradation 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, is performed within 31 days prior to startup and is only applicable to operating 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 3.3.1.12.

The CHANNEL FUNCTIONAL TEST for proper operation of the bypass permissives is critical during plant heatups because the operating 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 operating 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.

REFERENCES

1. DCD Tier 2, Section 7.3.
2. 10 CFR 50, Appendix A.
3. IEEE Standard 603-1991.
4. DCD Tier 2, Chapter 15.
5. 10 CFR 50.49.
6. DCD Tier 2, Section 7.2.

B 3.3 INSTRUMENTATION

B 3.3.6 Engineered Safety Features Actuation System (ESFAS) Logic and Manual Trip

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 Spray Actuation Signal (CSAS)
4. Main Steam Isolation Signal (MSIS)
5. Auxiliary Feedwater Actuation Signal SG #1 (AFAS-1)
6. Auxiliary Feedwater Actuation Signal SG #2 (AFAS-2)

Equipment actuated by each of the above signals is identified in the DCD Tier 2 (Reference 1).

The engineered safety features (ESF) system consists of four channels of sensors, APC-S cabinets, the ESFAS initiation portion of the PPS cabinets and ESF-CCS.

The ESFAS function is performed through the below portions in the ESF system.

a. Measurement channels

b. Bistable logic

c. ESFAS logic:

   – Coincidence Logic

   – Initiation Logic (trip paths)

   – Actuation Logic

BACKGROUND (continued)

This LCO addresses ESFAS logic. Bistable logic and measurement channel are addressed in LCO 3.3.5, “Engineered Safety Features Actuation System (ESFAS) Instrumentation.”

The role of the measurement channel and bistable logic is described in LCO 3.3.5. The role of the ESFAS logic is described below.

ESFAS Logic

The ESFAS logic, consisting of coincidence, initiation and actuation logic, employs a scheme that provides an ESF actuation of four divisions 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.

Coincidence Logic

There is one local coincidence logic (LCL) associated with each trip bistable logic of each channel. Each LCL receives four trip signals, one for its associated bistable logic in the channel and one from each of the equivalent bistable logic located in the other three channels. The LCL receives the trip channel bypass status associated with each of the above mentioned bistables. The function of the LCL is to generate a coincidence logic trip whenever two or more like bistables are in a tripped condition. The LCL takes into consideration the trip bypass input state when determining the coincidence logics state.

Designating the protection channels as A, B, C, D, with no trip bypass present, the LCL will produce a coincidence logic trip signal for any of the following trip inputs: AB, AC, AD, BC, BD, CD, ABC, ABD, ACD, BCD, ABCD. These represent all possible two- or more out-of-four trip combinations of the four protection channels. Should a trip bypass be present, the logic will provide a coincidence logic trip signal when two or more of the three un-bypassed bistables are in a tripped condition.

Initiation Logic

The initiation logic is designed to fail-safe. This will result in a partial trip (1 of 4) in the two-out-of-four ESFAS actuation logic. The partial trip will be alarmed the same as a full ESF trip and will be indicated by the QIAS and IPS; the partial trip cannot be bypassed.

BACKGROUND (continued)

Actuation Logic

The four initiation logic in the PPS actuate a two-out-of-four logic in the ESF-CCS. In the actuation logic, each signal also sets a latch when the two-out-of-four logic actuates to assure that the signal is not automatically reset once it has been initiated.

Receipt of two engineered safety system initiation channel signals will generate the actuation channel signals. This is done independently in each ESF-CCS cabinet, generating division A and division B and where required, division C and division D signals.

Manual Trip

Manual ESFAS Trip capability is provided to permit the operator to manually actuate an ESF system when necessary.

Two sets of two push buttons (in the MCR) for each ESF function are provided, and each set actuates the ESF of four trains (or two trains). Each manual trip push button signal is inputted to the actuation logic of ESF-CCS via control panel multiplexer (CPM). 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.

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 can be the primary actuation signal for more than one type of accident. An ESFAS Function can 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. The SIAS initiates the safety injection system and actuates the emergency diesel generator.

2. 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 a 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 during MSLBs or feedwater line breaks (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 a 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.

APPLICABLE SAFETY ANALYSES (continued)

5, 6. Auxiliary Feedwater Actuation Signal

AFAS consists of two steam generator specific signals (AFAS-1 and AFAS-2). AFAS-1 initiates auxiliary feed to SG #1 and AFAS-2 initiates auxiliary feed to SG #2.

AFAS maintains a steam generator heat sink during a small LOCA event, steam generator tube rupture event, MSLB, or FWLB event either inside or outside containment.

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.

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 occurs in Pressurizer Pressure – Low or Containment Pressure – High and is explained in Bases 3.3.5.

a. Coincidence Logic

This LCO requires four channels of SIAS coincidence logic to be OPERABLE in MODES 1, 2, 3, and 4.

b. Initiation Logic

This LCO requires four channels of SIAS initiation logic to be OPERABLE in MODES 1, 2, 3, and 4.

c. Actuation Logic

This LCO requires four channels of SIAS actuation logic to be OPERABLE in MODES 1, 2, 3, and 4.

d. Manual Trip

This LCO requires four channels of SIAS manual trip to be OPERABLE in MODES 1, 2, 3, and 4.

LCO (continued)

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. 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. Coincidence Logic

This LCO requires four channels of CSAS coincidence logic to be OPERABLE in MODES 1, 2, 3, and 4.

b. Initiation Logic

This LCO requires four channels of CSAS initiation logic to be OPERABLE in MODES 1, 2, 3, and 4.

c. Actuation Logic

This LCO requires four channels of CSAS actuation logic to be OPERABLE in MODES 1, 2, 3, and 4.

d. Manual Trip

This LCO requires four channels of CSAS manual trip to be OPERABLE in MODES 1, 2, 3, and 4.

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 coincidence logic. 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.

LCO (continued)

a. Coincidence Logic

This LCO requires four channels of CIAS coincidence logic to be OPERABLE in MODES 1, 2, and 3.

b. Initiation Logic

This LCO requires four channels of CIAS initiation logic to be OPERABLE in MODES 1, 2, and 3.

c. Actuation Logic

This LCO requires two channels of CIAS actuation logic to be OPERABLE in MODES 1, 2, 3, and 4.

d. Manual Trip

This LCO requires four channels of CIAS manual trip to be OPERABLE in MODES 1, 2, 3, and 4.

4. Main steam Isolation Signal (MSIS)

MSIS occurs on a Steam Generator Pressure – Low or Containment Pressure – High.

a. Coincidence Logic

This LCO requires six channels of coincidence logic to be OPERABLE in MODES 1, 2, 3, and 4.

b. Initiation Logic

This LCO requires four channels of initiation logic to be OPERABLE in MODES 1, 2, 3, and 4.

c. Actuation Logic

This LCO requires four channels of actuation logic to be OPERABLE in MODES 1, 2, 3, and 4.

d. Manual Trip

This LCO requires four channels of manual trip to be OPERABLE in MODES 1, 2, 3, and 4.

LCO (continued)

5. Auxiliary Feedwater Actuation Signal SG #1 (AFAS-1)

AFAS-1 occurs on a Steam Generator Level – Low in Steam Generator #1.

a. Coincidence Logic

This LCO requires four channels of coincidence logic to be OPERABLE in MODES 1, 2, and 3.

b. Initiation Logic

This LCO requires four channels of initiation logic to be OPERABLE in MODES 1, 2, and 3.

c. Actuation Logic

This LCO requires four channel of actuation logic to be OPERABLE in MODES 1, 2, 3, and 4.

d. Manual Trip

This LCO requires four channels of manual trip to be OPERABLE in MODES 1, 2, 3, and 4.

6. Auxiliary Feedwater Actuation Signal SG #2 (AFAS-2)

AFAS-2 occurs on a Steam Generator Level – Low in Steam Generator #2.

a. Coincidence Logic

This LCO requires six channels of coincidence logic to be OPERABLE in MODES 1, 2, and 3.

b. Initiation Logic

This LCO requires four channels of initiation logic to be OPERABLE in MODES 1, 2, and 3.

c. Actuation Logic

This LCO requires four channel of actuation logic to be OPERABLE in MODES 1, 2, 3, and 4.

LCO (continued)

d. Manual Trip

This LCO requires four channels of manual trip to be OPERABLE in MODES 1, 2, 3, and 4.

7. Diverse Manual ESF Actuation Signal

The diverse manual ESF actuation interface to ESF components is initiated manually from switches in the MCR. The switches for safety injection, containment spray, auxiliary feedwater, main steam isolation, and containment isolation have two positions as follows: normal and actuate. When in actuate, input received from the network communication interface to actuate the components will be overridden.

This LCO requires two channels of safety injection, containment spray, auxiliary feedwater, and one channel for each main steam isolation valve and one channel for containment isolation to be OPERABLE in MODES 1, 2, 3, and 4.

APPLICABILITY

In MODES 1, 2, 3 and 4, there is sufficient energy in the primary and secondary systems to warrant automatic ESF System responses to:

a. Close the main steam isolation valves to preclude a positive reactivity addition.

b. Actuate auxiliary feedwater to preclude the loss of the steam generators as a heat sink (in the event the normal feedwater system is not available).

c. 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.

d. 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 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.

The ESFAS manual trip capability is required in MODE 4 for SIAS, CIAS, CSAS, MSIS and AFAS 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.

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.

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.

ACTIONS (continued)

A.1

Condition A applies to one manual trip, coincidence logic, 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 affects one leg of two-out-of-four actuation logic channel. In this case, according to the purpose of operation Technical Specification, actuation logic is not inoperable status. When initiation logic channel is failure, LCO 3.0.3 may be not entered. This Action is different from Required Action related to the RPS Manual channel inoperable because open contact of reactor trip switchgear is implemented and confirmed easily in RPS. If the channel cannot be restored to OPERABLE status with 48 hours, Condition E or F is entered.

B.1 and B.2

Condition B 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 coincidence logic or vital bus power failure.

If a LCL power supply or vital instrument bus is lost, the initiation logic channels in the same trip leg will generate the initiation signal. This will open the actuation logic contacts, satisfying the Required Action to generate at least the actuation logic signal in the affected trip leg from actuation logic.

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 initiation logic is low during any given 48 hour period.

ACTIONS (continued)

If the channel cannot be restored to OPERABLE status with 48 hours, Condition E or F is entered.

Of greater concern is the failure of the initiation circuit in a non-trip condition (e.g., two initiation logic failures). With one failed, there is still the redundant input in the trip leg of each two-out-of-four 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 actuation logic signal in the affected trip leg is required. If the required actuation logic signal has not occurred, as indicated by annunciation or trip leg current lamps, manual trip of the affected trip leg may be attempted. Caution must be exercised since depressing the wrong ESFAS push buttons can result in an ESFAS actuation.

C.1

Condition C 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 could 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. If the channel cannot be restored to OPERABLE status with 48 hours, Condition E or F is entered.

Failure of a single initiation logic channel, coincidence logic power supply, or vital instrument bus could 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, coincidence, or initiation channel failure.

Required Action C.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.

ACTIONS (continued)

D.1

The Required Action D applies to the diverse manual ESF Actuation equipment.

The associated Completion Time and LCO are reasonable based on operating experience for repair and restoration of this type of diverse manual ESF equipment In addition, it is assumed that a low probability for a multiple failures in the automatic ESFAS actuation logic and other manual controls within 72 hours will occur. If the inoperable channel is not restored to OPERABLE status within 72 hours, it is entered to the Condition F.

E.1 and E.2

If the Required Actions and associated Completion Times for the Condition 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 the Required Actions and associated Completion Times for the Condition 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

Since the ITP does not perform the safety related functions of ESFAS, the OPERABILITY is not limited by LCO 3.3.6. But, ITP must maintain the functional integrity for operation of CHANNEL FUNCTIONAL TEST.

SR 3.3.6.1

A CHANNEL FUNCTIONAL TEST is performed every 31 days to ensure the entire channel will perform its intended function when needed. The operability of the each channel or automatic actuation logic channel is verified by the operator every 31 days at least to meet the surveillance requirement.

The CHANNEL FUNCTIONAL TEST is part of an overlapping test sequence similar to that employed in the RPS. This sequence, consisting of SRs 3.3.5.2, 3.3.6.1, and 3.3.6.2 tests the entire ESFAS from the bistable input through the actuation of the individual subgroup. These overlapping tests are described in Reference 1. SRs 3.3.5.2 and 3.3.6.1 are normally performed together and in conjunction with ESFAS testing. When actuation signal of each subgroup is generated, SR 3.3.6.2 verifies the actuation ability of ESF component associated actuation signal of the associated each subgroup.

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 LCL testing, initiation logic (trip path) testing, and actuation logic testing.

Local Coincidence Logic Testing

LCL testing is tested to verify the operability of two-out-of-four logic and trip channel bypass logic.

Initiation Logic (Trip Path) Testing

Initiation logic testing is for Initiation Logic which consists of logical “OR”, and performed after the completion of LCL testing. This testing implements the only one Initiation logic of one channel at a time.

Actuation Logic Testing

Actuation logic testing is tested to verify the operability of two-out-of-four actuation logic after the completion of initiation logic (trip path) testing. This test is performed only for one channel and one actuation logic by periodic automatic test.

SURVEILLANCE REQUIREMENTS (continued)

Manual ESF Actuation Testing

Manual ESF actuation testing is tested every 31 days to verify that manual pushbutton can actuate the actuation logic as designed.

The 31-day Surveillance period is determined by operating experience and shows that equipment can meet the Surveillance requirement condition when equipment is tested as this Surveillance period.

SR 3.3.6.2

Individual subgroup must also be tested, one at a time, to verify the individual ESFAS components will actuate when required.

The 31-day Frequency on a staggered test basis complies with the operating experience and ensures the problems of individual logic signal can be detected within this time frame.

Some components cannot be tested at power operation since their actuation may lead to plant trip or equipment damage. Actuation logic subgroups not tested at power operation must be tested in accordance with the Note to this SR.

SR 3.3.6.3

A CHANNEL FUNCTIONAL TEST for diverse ESF manual actuation channel performs the diverse manual ESF actuation circuit by manual actuation of each Function. This testing is performed every 18 months to verify that the trip pushbutton can actuate the actuation logic as designed.

REFERENCES

1. DCD Tier 2, Section 7.3.

B 3.3 INSTRUMENTATION

B 3.3.7 Emergency Diesel Generator (EDG) – Loss of Voltage Start (LOVS)

BASES

BACKGROUND

The EDGs 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 “Onsite Power Systems” (Reference 1).

Trip Setpoints and Allowable Values

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 Setpoint Control Program (SCP) 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 SCP. 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.

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 EDG starts and is available to accept loads within a 17-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 (Reference 2).

Since there are four protective channels in a two-out-of-four trip logic for each train of the 4.16 kV power supply, no single failure will cause or prevent protective system actuation. This arrangement meets IEEE Std 603 criteria (Reference 3).

APPLICABLE SAFETY ANALYSES

The EDG – 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 EDG based on a loss of offsite power during a loss of coolant accident. The actual EDG 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 EDG supplied power following a loss of offsite power. The analysis assumes a non-mechanistic EDG 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 EDG start, EDG loading, and safety injection system component actuation. The response of the EDG 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 EDGs, 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 10 CFR 50, Appendix A, GDC 21 (Reference 4).

APPLICABLE SAFETY ANALYSES (continued)

The delay times assumed in the safety analysis for the ESF equipment include the 17-second EDG 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 EDG loading and sequencing delay.

The EDG – 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 EDG 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 EDG is required to be OPERABLE to ensure that the automatic start of the EDG 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 EDG 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.

Allowable Values and nominal trip setpoints are specified for each Function in the LCO in the SCP. 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 SCP.

BASES

LCO (continued)

A channel is inoperable if its actual trip setpoint is not within its required Allowable Value.

APPLICABILITY

The EDG – 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 EDG 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 non-conservative 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 EDG 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 EDG – LOVS Function. The Completion Times of the inoperable channels of a Function will be tracked separately for each Function, starting from the time the Condition was entered for that Function.

ACTIONS (continued)

A.1 and A.2

Condition A applies if one channel is inoperable for one or more Functions per EDG 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).

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.

B.1 and B.2

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 Action for the associated EDG made inoperable by EDG – 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.

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 EDG – LOVS channel, and placing a second channel in trip will result in a loss of voltage diesel start signal. Therefore, if one EDG – 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.

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 EDG – 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 EDG 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 EDG – LOVS Function.

SR 3.3.7.1

Performance of the CHANNEL CHECK 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.

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 to ensure that the entire CHANNEL will perform its intended function when needed. A successful test of the required contacts 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 (TS) and non-TS tests at least once per refueling interval with applicable extensions.

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. The SCP has controls which require verification that the instrument channel functions as required by verifying the as-left and as-found setting are consistent with those established by the setpoint methodology.

SR 3.3.7.3

SR 3.3.7.3 is the performance of a CHANNEL CALIBRATION. 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. The SCP has controls which require verification that the instrument channel functions as required by verifying the as-left and as-found setting are consistent with those established by the setpoint methodology.

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. DCD Tier 2, Chapter 8.
2. DCD Tier 2, Chapter 15.
3. IEEE Standard 603-1991.
4. 10 CFR 50, Appendix A, GDC 21.

B 3.3 INSTRUMENTATION

B 3.3.8 Containment Purge Isolation Actuation Signal (CPIAS)

BASES

BACKGROUND

This LCO encompasses the CPIAS, 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 actuation,” or LCO 3.3.7, “Emergency Diesel Generator (EDG) – Loss of Voltage Start (LOVS).” Individual plants shall include the CPIAS Function and LCO requirements that are applicable to them.

The CPIAS provides protection from radioactive contamination in 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 CPIAS 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 low and high volume purge supply and exhaust valves are closed on a CPIAS when a high radiation level in containment is detected.

The CPIAS includes two independent, redundant logic subsystems, including actuation trains. Each train employs two sensors, each one detecting gamma (area).

If any one of these sensors exceeds the bistable trip setpoint, the CPIAS train will be actuated (one-out-of-two 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).

<u>Actuation Setpoints and Allowable Values</u>

Actuation setpoints used in the bistables are based on the analytical limits (Reference 1). The selection of these actuation setpoints is such that adequate protection is provided when all sensor and processing time delays are taken into account.

BACKGROUND (continued)

To allow for calibration tolerances, instrumentation uncertainties, and instrument drift, actuation setpoint Allowable Values specified in the setpoint control program (SCP) are conservatively adjusted with respect to the analytical limits. The actual nominal actuation 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 CPIAS 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 CPIAS is also required to close the containment purge valves in the event of the fuel handling accident in containment, as described in Reference 1. This accident is a limiting case representing a class of accidents that may involve radiation release in containment without CIAS actuation. The CPIAS ensures the consequences of a dropped fuel assembly in containment are not as severe as a dropped assembly in the fuel handling area. This ensures that the offsite consequences of radiation accidents in containment are within 10 CFR 50.34 limits (Reference 2).

The CPIAS satisfies the requirements of LCO Selection Criterion 3.

LCO

LCO 3.3.8 requires one CPIAS channel to be OPERABLE. The required channel consists of area radiation monitors, actuation logic; and manual actuation.

The specific Allowable Values for the setpoints of the CPIAS are listed 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 actuation setpoint and the Allowable Value is equal to or greater than the drift allowance assumed for each actuation 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 actuation function.

The bases for the LCO on CPIAS are discussed below for each Function:

a. manual actuation

The LCO on manual actuation backs up the automatic actuation and ensures operators have the capability to rapidly initiate the CPIAS Function if any parameter is trending toward its setpoint. Only one manual channel of CPIAS is required in MODES 1, 2, 3, and 4, since the CPIAS is redundant with the CIAS and SIAS. Only one manual channel of CPIAS 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. Containment Area Radiation

The LCO on the radiation channels requires that each channel be OPERABLE for each actuation logic channel.

The actuation setpoint is selected to allow detection of small deviations from normal. The absolute value of the actuation 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 radiation level expected in these MODES.

LCO (continued)

c. actuation logic

One channel of actuation logic is required, since the valves can be shut independently of the CPIAS signal either manually from the MCR or using either the SIAS or CIAS push button.

APPLICABILITY

In MODES 1, 2, 3, and 4, the low volume purge values 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 CORE ALTERATIONS or movement of irradiated fuel assemblies within containment, there is the possibility of a fuel handling accident requiring CPIAS on high radiation in containment.

The APPLICABILITY is modified by a Note, which states that the CPIAS Specification is only required when the penetration is not isolated by at least one closed and deactivated automatic valve, closed manual valve, or blind flange.

ACTIONS

A CPIAS 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 actuation 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 actuation 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.

ACTIONS (continued)

When the number of inoperable channels in a actuation Function exceeds that specified in any related Condition associated with the same actuation 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 CPIAS manual actuation, actuation logic, and required 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 MODE 5 within 36 hours.

C.1, C.2.1, and C.2.2

Condition C applies to the same conditions as are described in Condition A; however, the applicability is during CORE ALTERATIONS or during the movement of 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 CPIAS. Required Actions C.2.1 and C.2.2 may be performed in lieu of Required Action C.1. Required Action C.2.1 requires the suspension of CORE ALTERATIONS and Required Action C.2.2 requires suspension of movement of 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 CPIAS provides the only automatic mitigation of radiation release.

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 upper operating area radiation monitor channels used in the CPIAS. 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 could be an indication that the transmitter or the signal processing equipment has drifted outside its limit.

The Surveillance 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 operating area monitor channels used in the CPIAS. It differs only in the Frequency as weekly. This technique results in an integration of total operating area radiation activity until the assemblies are replaced. The low levels of activity expected make more frequent monitoring unnecessary.

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. The SCP has controls which require verification that the instrument channel functions as required by verifying the as-left and as-found setting are consistent with those established by the setpoint methodology. 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 applicable 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. The SCP has controls which require verification that the instrument channel functions as required by verifying the as-left and as-found setting are consistent with those established by the setpoint methodology. 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 applicable during CORE ALTERATIONS or during movement of irradiated fuel assemblies within containment.

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 Note to the SR indicates that this Surveillance includes verification of operation for each initiation relay.

SURVEILLANCE REQUIREMENTS (continued)

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.

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 3.3.8.7

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 CPIAS manual actuation channel.

This test verifies that the actuation 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.

REFERENCES

1. DCD Tier 2, Chapter 15.

2. 10 CFR 50.34.

B 3.3 INSTRUMENTATION

B 3.3.9 Control Room Emergency Ventilation Actuation Signal (CREVAS)

BASES

BACKGROUND

This LCO encompasses CREVAS 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 actuation,” or LCO 3.3.7, “Emergency Diesel Generator (EDG) – Loss of Voltage Start (LOVS).” This is a BOP 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 CREVAS terminates the normal supply of outside air to the MCR and initiates actuation of the control room emergency air cleaning unit to minimize operator radiation exposure. The CREVAS includes two independent, redundant subsystems, including actuation trains. Each train employs two separate sensors and detects gaseous activity. 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).

Actuation Setpoints and Allowable Values

Actuation setpoints used in the bistables are based on the analytical limits (Reference 1). The selection of these actuation 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 the setpoint control program (SCP) are conservatively adjusted with respect to the analytical limits. The actual nominal actuation 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.

BACKGROUND (continued)

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 the main control room (MCR) dose is 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 CREVAS, in conjunction with the control room area HVAC System maintains the MCR atmosphere within conditions suitable for prolonged occupancy throughout the duration of any one of the accidents discussed in Reference 1. The radiation exposure of MCR personnel, through the duration of any one of the postulated accidents discussed in "Transient and Accident Analysis," DCD Tier 2, Chapter 15 (Reference 1), does not exceed the limits set by 10 CFR 50, Appendix A, GDC 19 (Reference 2).

The CREVAS satisfies the requirements of LCO SELECTION CRITERION 3.

LCO

LCO 3.3.9 requires one channel of CREVAS to be OPERABLE. The required channel consists of actuation logic, manual actuation, and gaseous radiation monitors. The specific Allowable Values for the setpoints of the CREVAS are listed in the SRs.

Operation with an actuation setpoint less conservative than the nominal actuation setpoint, but within its allowable value, is acceptable provided that the difference between the nominal actuation setpoint and the allowable value is equal to or greater than the drift allowance assumed for each actuation in the transient and accident analyses.

LCO (continued)

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 actuation function. A channel is inoperable if its actual actuation setpoint is not within its required Allowable Value.

The bases for the LCO on the CREVAS are discussed below for each Function:

a. manual actuation

The LCO on manual actuation backs up the automatic actuation and ensures operators have the capability to rapidly initiate the CREVAS Function if any parameter is trending toward its setpoint. One channel must be OPERABLE. This considers that the manual actuation capability is a backup and that other means are available to actuate the redundant train if required, including manual SIAS.

b. Gaseous Radiation

Both channels of gaseous radiation detection in the required train are required to be OPERABLE to ensure the MCR isolates on high gaseous concentration.

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 CREVAS Functions must be OPERABLE in MODES 1, 2, 3, and 4, during CORE ALTERATIONS, and during movement of irradiated fuel assemblies to ensure a habitable environment for the MCR operators.

ACTIONS

A CREVAS 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 actuation 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, C.2.2, and C.2.3

Conditions A, B, and C are applicable to manual and automatic actuation of the control room area HVAC system by CREVAS. Condition A applies to the failure of the CREVAS manual actuation, actuation logic, 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 CREVAS 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 CREVAS supplements MCR 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.

Condition C applies to the failure of CREVAS manual actuation, actuation logic, and required gaseous monitor channels during CORE ALTERATIONS or when moving irradiated assemblies. The Required Actions are immediately taken to place one OPERABLE control room area HVAC system train in the emergency radiation protection mode, or to suspend CORE ALTERATIONS, positive reactivity additions, and movement of irradiated fuel assemblies.

ACTIONS (continued)

The Completion Time recognizes the fact that the radiation signals are the only Functions available to initiate MCR isolation in the event of a fuel handling accident.

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 could 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.

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.9.2

A CHANNEL FUNCTIONAL TEST is performed on the required MCR radiation monitoring channel to ensure the entire channel will perform its intended function.

The SCP has controls which require verification that the instrument channel functions as required by verifying the as-left and as-found setting are consistent with those established by the setpoint methodology.

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.

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.

Note indicates this Surveillance includes verification of operation for each initiation relay.

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. The SCP has controls which require verification that the instrument channel functions as required by verifying the as-left and as-found setting are consistent with those established by the setpoint methodology. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drift between successive calibrations to ensure that the channel remains operational between successive surveillances.

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 3.3.9.5

Every 18 months, a CHANNEL FUNCTIONAL TEST is performed on the manual CREVAS actuation channel.

This test verifies that the actuation 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.

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. DCD Tier 2, Chapter 15.

2. 10 CFR 50, Appendix A, GDC 19.

B 3.3 INSTRUMENTATION

B 3.3.10 Fuel Handling Area Emergency Ventilation Actuation Signal (FHEVAS)

BASES

BACKGROUND

This LCO encompasses FHEVAS, 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 Actuation,” or LCO 3.3.7, “Emergency Diesel Generator (EDG) – Loss of Voltage Start (LOVS).” This is a BOP 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 FHEVAS provides protection from radioactive contamination in the spent fuel pool area in the event that a spent fuel element ruptures during handling.

The FHEVAS 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 FHEVAS includes two independent, redundant subsystems, including actuation trains. Each sensing channel employs one separate sensor. Since there is a separate sensor in each sensing channel, the actuation trains are redundant. If the bistable monitoring either sensor indicates an unsafe condition, the redundant actuation trains will be actuated through one-out-of-two logic coincidence logic. The two trains actuate separate equipment.

Actuation Setpoints and Allowable Values

Actuation setpoints used in the bistables are based on the analytical limits (Reference 2). The selection of these actuation 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 the setpoint control program are conservatively adjusted with respect to the analytical limits. The actual nominal actuation 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.

BACKGROUND (continued)

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 FHEVAS is required to isolate the normal fuel handling area HVAC system and automatically initiate the recirculation and filtration systems in the event of the fuel handling accident in the fuel handling area, as described in Reference 2. The FHEVAS helps ensure acceptable consequences for the dropping of a spent fuel bundle breaching up to 60 fuel pins.

The FHEVAS satisfies the requirements of LCO SELECTION CRITERION 3.

LCO

LCO 3.3.10 requires one channels of FHEVAS to be OPERABLE. The required channel consists of actuation logic, manual actuation, and area radiation monitors. The specific Allowable Values for the setpoints of the FHEVAS are listed in the SRs.

Only the Allowable Values are specified for each actuation Function in the SRs. Operation with an actuation setpoint less conservative than the nominal actuation setpoint, but within its allowable value, is acceptable, provided that the difference between the nominal actuation setpoint and the Allowable Value is equal to or greater than the drift allowance assumed for each actuation 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 actuation Function.

LCO (continued)

The Bases for the LCO on the FHEVAS are discussed below for each Function:

a. Manual actuation

The LCO on manual actuation ensures that the FHEVAS Function can easily be initiated if any parameter is trending rapidly toward its setpoint. Components can be actuated independently of the FHEVAS. Both available channels are required to ensure a single failure will not disable automatic initiation capability.

b. Area Radiation

The LCO on the two area radiation channels requires that each channel be OPERABLE for the required actuation logic.

c. Actuation logic

Two channels of actuation logic are required to be OPERABLE to ensure no single random failure can prevent automatic actuation.

APPLICABILITY

The FHEVAS Functions are required to be OPERABLE during movement of irradiated fuel in the fuel handling area. The FHEVAS isolates the fuel handling area in the event of a fuel handling accident.

The FHEVAS must be OPERABLE in during movement of irradiated fuel in the fuel handling area, since the FHEVAS isolates the fuel handling area in the event of a fuel handling accident.

ACTIONS

An FHEVAS 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 actuation 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 actuation setpoint is found non-conservative 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 an actuation Function exceeds that specified in any related Condition associated with the same actuation 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 only to those configurations when the fuel handling area HVAC is shared with the ESF equipment room.

Condition A applies to any FHEVAS manual actuation, actuation logic, and radiation monitors inoperable during movement of irradiated fuel in the fuel handling area.

The Required Actions place one OPERABLE fuel handling area HVAC system train in operation or suspend movement of irradiated fuel in the fuel handling area. These Required Actions are required to be completed immediately.

The Completion Time accounts for the higher likelihood of releases in the fuel handling area during fuel handling.

SURVEILLANCE REQUIREMENTS

SR 3.3.10.1

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 could 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 checks channel OPERABILITY during normal operational use of the displays associated with the LCO required channels.

SR 3.3.10.2

A CHANNEL FUNCTIONAL TEST is performed on the required fuel handling area radiation monitoring channel to ensure the entire channel will perform its intended function. The SCP has controls which require verification that the instrument channel functions as required by verifying the as-left and as-found setting are consistent with those established by the setpoint methodology.

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.

SURVEILLANCE REQUIREMENTS (continued)

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. 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.

SR 3.3.10.4

Every 18 months, a CHANNEL FUNCTIONAL TEST is performed on the FHEVAS manual actuation channel.

This Surveillance verifies that the actuation 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.

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. The SCP has controls which require verification that the instrument channel functions as required by verifying the as-left and as-found setting are consistent with those established by the setpoint methodology.

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.

SURVEILLANCE REQUIREMENTS (continued)

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.

REFERENCES

1. DCD Tier 2, Chapter 9.

2. DCD Tier 2, Chapter 15.

B 3.3 INSTRUMENTATION

B 3.3.11 Accident Monitoring Instrumentation (AMI)

BASES

BACKGROUND

The primary purpose of the AMI is to display plant variables that provide information required by the main control room (MCR) operators during accident situations.

The OPERABILITY of AMI 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 AMI is important so that responses to corrective actions can be observed, and the need for further actions can be determined. These essential instruments are identified in DCD Tier 2, Chapter 7 (Reference 1) addressing the recommendations of NRC RG 1.97 (Reference 2), as required by Supplement 1 to NUREG-0737, “TMI Action Items” (Reference 3).

The AMI instruments included in Table 3.3.11-1, Accident Monitoring Instrumentation, are required for the following reasons:

- Perform the diagnosis specified in the emergency operating procedures. These variables are restricted to preplanned actions for the primary success path of DBAs (e.g., loss-of-coolant accident [LOCA]).

- Provide information to indicate whether plant safety functions are being accomplished for reactivity control, core cooling, maintaining reactor coolant system integrity, and maintaining containment integrity (including radioactive effluent control).

- Provide information to indicate the potential for being breached or actual breach of the barriers to fission product releases (i.e., fuel cladding, primary coolant pressure boundary, and containment).

- Provide information to indicate the performance of those safety systems and auxiliary supporting features necessary for the mitigation of design basis events and to indicate the performance of other systems necessary to achieve and maintain a safe shutdown condition and to verify safety system status.

BACKGROUND (continued)

- Provide information to indicate the magnitude of the release of radioactive materials and to assess such releases. The AMI is displayed through the qualified indication and alarm system (QIAS).

APPLICABLE SAFETY ANALYSIS

The AMI ensures the OPERABILITY of NRC RG 1.97 variables, so that the MCR 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.
- 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.
- 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.
- Initiate action necessary to protect the public as well as to obtain an estimate of the magnitude of any impending threat.

AMI that performs certain functions related to verification of key safety functions and monitoring key barriers for breach must be retained in the Specification because they are intended to assist operators in minimizing the consequences of accidents. Therefore, these variables are important in reducing public risk.

The seismically qualified indication and alarm system - P (QIAS-P) is dedicated to continuously monitor and display the Type A, B, and C variables. Type A variables are displayed as conventional indicators on the safety console. The qualified indication and alarm system - non-safety(QIAS-N) and information processing system (IPS) also monitor all Type A, B, C, D, and E variables.

APPLICABLE SAFETY ANALYSIS (continued)

Two measurement CHANNELS provide the necessary information in the MCR for adequate accident monitoring. The CHANNELS provide wide-range information which meets the electrical and physical separation requirements for each parameter displayed. This design is consistent with the requirements of IEEE Std. 603-1991 (Reference 4). The CHANNELS are provided with equipment qualified to operate in the environments specified for design basis events. These CHANNELS comply with the recommendations of NRC RG 1.97.

LCO

LCO 3.3.11 requires two OPERABLE MEASUREMENT 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 could be required at some plants if the NRC RG 1.97 analysis determined that failure of one accident monitoring channel results in information ambiguity (that is, the redundant display disagree) that could lead operator to defeat or to fail to accomplish a required safety function.

The exception to the two CHANNEL requirement is the 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 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.

LCO (continued)

Listed below are discussions of the specified instrument functions listed in Table 3.3.11-1. The following instruments are displayed on QIAS-P, QIAS-N, and IPS.

1. Logarithmic Reactor Power

Logarithmic Reactor Power indication is provided to verify reactor shutdown.

Inputs are provided by two safety CHANNELS with a minimum sensor and indicated range of 2×10^{-8} to 100 % power.

2, 3. Reactor Coolant Hot Leg Temperature (wide range) and Cold Leg Temperature (wide range)

Reactor coolant hot leg and cold leg temperatures are variables provided for verification of core cooling and long term surveillance. They are also inputs to the reactor coolant system subcooled margin monitor.

Reactor coolant outlet and inlet temperature inputs to the AMI are provided by two fast response resistance elements and associated transmitters in each loop. The CHANNELS provide indication over a minimum sensor and indicated range of 0 to 400°C (32 to 752 °F).

4. Reactor Coolant System Pressure (wide range)

RCS pressure (wide range) is a 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 minimum sensor and indicated range of 0 to 281.2 kg/cm^{2}G (4,000 psig). The pressure transmitters are located inside the containment. Redundant monitoring capability is provided by two trains of instrumentation.

LCO (continued)

5. Reactor Vessel Coolant Level

Reactor vessel coolant level is provided for verification and long term surveillance of core cooling.

The reactor vessel coolant level monitors provide a direct measurement of the collapsed liquid level above the core support surface. The collapsed liquid represents the amount of liquid mass that is in the reactor vessel above the core. Measurement of the collapsed coolant level is selected because it is a direct indication of the coolant 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 can occur during the preceding core recovery interval.

The level range extends from the top of the vessel down to the top of the core support surface. 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 core support surface. 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.

Two CHANNELS with minimum sensor range of 0 to 939.8 cm (0 to 370 in) above the core support surface is provided. The minimum indicated range for these two CHANNELS is 0 to 100 %.

6. Reactor Cavity Level

Reactor cavity level is provided for verification and long term surveillance of the RCS integrity and vessel integrity.

Reactor cavity level is measured by four instruments with a minimum sensor and indicated range of 0 to 100 %.

LCO (continued)

7, 8. Containment Pressure (wide range, extended wide range)

Containment pressure (wide range, extended wide range) is provided for verification of RCS and containment OPERABILITY.

Two extended wide range pressure sensors with a minimum sensor and indicated range of –500 to 14, 500 cmH_2O (–7.1 to 206.2 psig) and two wide range sensors with a minimum sensor and indicated range of –400 to 5,600 cmH_2O (–5.7 to 79.5 psig) are provided for display of related information.

9. Containment Isolation Valve Position

Containment Isolation Valve Position is provided for verification of containment isolation OPERABILITY.

Containment Isolation Valve Position indication is summarized by two status indicators. The containment isolation valves are split between the two status indicators in cases where there are two containment isolation valves for one penetration. For any particular containment penetration, one isolation valve or boundary is on one status indicator, and the other isolation valve or boundary is on the other status indicator. These status indicators will identify if any single Containment Isolation Valve is not in its required position (closed) for isolation valves aggregated under that status indicator. Any Containment Isolation Valve whose associated penetration is isolated by at least one closed and deactivated automatic valve, closed manual valve, blind flange, or check valve with flow through the valve secured will not cause the associated Containment Isolation Valve status indicator to indicate that not all of the Containment Isolation Valves are closed, if all other Containment Isolation Valves associated with that indicator closed. Required inputs, to the Containment Isolation Valve position status algorithm include 1 pair of closed/not closed valve position indication for each Containment Isolation Valve.

LCO (continued)

10. Containment Upper operating Area Radiation

The Containment Upper operating Area Radiation monitor 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. Two sensors with a minimum sensor and indicated range of 10^1 to 10^8 mSv/hr provide input to the monitor.

11. Pressurizer Level

The 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 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.

Two pressurizer level sensors are provided. They have a minimum indicated and sensor range of 0 to 100 %.

12. Steam Generator Level (wide range)

The Steam Generator Level (wide range) monitor is provided to monitor operation of decay heat removal via the steam generators. The measured differential pressure is displayed as 0 to 100 % at the reference leg temperature of 20 °C (68 °F). Temperature compensation of this indication is performed manually by the operator. Redundant monitoring capability is provided by two trains of instrumentation.

LCO (continued)

13. Holdup Volume Tank (HVT) Level

The HVT performs water collection and storage functions during accident conditions. Level indication is provided in the MCR to allow the operator to monitor HVT level after an accident. HVT level is measured by five instruments with a minimum sensor and indicated range of 0 to 100 %.

14, 15, 16, 17. Core Exit Temperature

Core exit temperature is provided for verification and long term surveillance of core cooling.

An evaluation is made of the minimum number of valid core exit thermocouples necessary for inadequate core cooling detection. The evaluation determines 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 incore instrument detector assemblies. The junction of each thermocouple is located a few inches (cm) 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 sensor and indicated temperature range from 0 to 1,260.0 ^{o}C (32 to 2,300 °F), although accuracy is reduced at temperatures above 982.2^{o}C (1,800 °F).

LCO (continued)

18. Steam Generator Pressure

The Steam Generator Pressure monitor is provided to monitor operation of the Steam Generators and verification of RCS heat removal. There are two sensed CHANNELS of the Steam Generator Pressure per Steam Generator. The minimum sensor range of these CHANNELS is 1.1 to 105.5 kg/cm^2 A (15 to 1500 psia). The minimum indicated range of these CHANNELS is 0 to 105 kg/cm^2A (0 to 1494 psia).

19. Degree of Subcooling

Degree of subcooling is provided for verification and analysis of plant conditions.

There are two sensed CHANNELS of degree of subcooling. Degree of subcooling is calculated from the following instruments: Wide Range Pressurizer Pressure (minimum sensor range of 0 to 210.9 kg/cm^2A [0 to 3,000 psia]), Reactor Coolant Hot Leg and Cold Leg Temperatures (Minimum Sensor Range of 0 to 400 ^oC [32 to 752 °F]), and Core Exit Temperatures (Minimum Sensor Range of 0 to 1,260.0 ^oC [32 to 2,300 °F]). The degree of subcooling indicated range is a minimum of 93.3 ^oC (200 °F) subcooling to 1.7 ^oC (35 °F) superheat.

20. Pressurizer Pressure (wide range)

Pressurizer Pressure (wide range) is measured by pressure transmitters with a minimum sensor and indicated range of 0 to 210.9 kg/cm^2A (0 to 3,000 psia).

LCO (continued)

21. IRWST Level

The IRWST Level monitor is provided to sure water supply for Emergency Core Cooling and Containment Spray. The IRWST consists of one torus-type tank inside containment. There are four 0 to 100 % sensors and indicated range level CHANNELS.

22. IRWST Temperature

IRWST temperature is provided for verification of long term decay heat removal operation. There are four 50 to 350 °F sensors with an indicated range temperature CHANNELS.

23. Containment Level

The containment level monitor is provided for verification and long term surveillance of Emergency Core Cooling and the Containment Level is measured by two instruments with a minimum sensor and indicated range of 0 to 100 %.

24. Control Rod Position

To verify whether the Control Rods are full in or not full in, Control Rod Positions are calculated in CPCS with a range of 0 to 381 cm.

25. Containment Operating Area Radiation

A containment operating area radiation monitor is provided to monitor the potential of significant radiation releases from an event occurring in the containment (e.g., fuel handling accident) and to provide a release assessment for use by operators in determining the need to invoke the site emergency plans. In addition, this area monitoring initiates containment purge isolation actuation signal (CPIAS) to prevent radioactive release through containment purge system.
Two containment operating radiation monitors are available and two sensors with a minimum sensor indicated range of 10^{-3} mSv/hr to 10^{2} mSv/hr provide input

LCO (continued)

26. Spent Fuel Pool Radiation

The spent fuel pool radiation monitor is provided to monitor the potential of significant radiation releases from the event occurring in the fuel handling area (e.g., fuel handling accident) and to provide release assessment for use by operators in determining the need to invoke site emergency plans. In addition, this area monitor initiates fuel handling area emergency ventilation actuation signal (FHEVAS) to stop the fuel handling area normal ventilation system and to activate the fuel handling area emergency ventilation system. Two spent fuel pool radiation monitors are available and two sensors with a minimum sensor indicated range of 10^{-3} mSv/hr to 10^{2} mSv/hr provide input.

Two CHANNELS are required to be OPERABLE for all but one Function. Two OPERABLE CHANNELS ensure that no single failure within the AMI 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 obtaining 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 delineates that the exception to the two CHANNEL requirements is the 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 is 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 indicates the radial temperature gradient across their core quadrant. 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 passive valve or 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 AMI 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 AMI is low; therefore, the AMI is not required to be OPERABLE in these MODES.

ACTIONS

Note 1 has been added in the ACTIONS to exclude the MODE change restriction of LCO 3.0.4. This exception allows entry into the applicable MODE while relying on the ACTIONS, even though the ACTIONS may eventually require plant shutdown. This exception is acceptable due to the passive function of the instruments, the operator's ability to monitor an accident using alternate instruments and methods, and the low probability of an event requiring these instruments.

Note 2 has been added in the ACTIONS to clarify the application of Completion Time rules. The Condition 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 MEASUREMENT CHANNEL that is inoperable, the required inoperable CHANNEL must be restored to OPERABLE status within 31 days. The 31-day Completion Time is based on operating experience and takes into account the remaining OPERABLE MEASUREMENT CHANNEL (or in the case of a Function that has only one required

ACTIONS (continued)

MEASUREMENT CHANNEL, other non NRC RG 1.97 instrument MEASUREMENT 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 AMI 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 NRC. 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 measurement CHANNELS inoperable (i.e., two measurement CHANNELS inoperable in the same Function), one measurement 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 AMI 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 AMI.

Therefore, requiring restoration of one inoperable CHANNEL of the Function limits the risk that the AMI 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.

ACTIONS (continued)

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 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

Alternate means of monitoring Reactor Vessel Coolant Level and Containment Area Radiation have been developed and tested. These alternate means may be temporarily installed if the normal accident monitoring 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 accident monitoring channels, justify the areas in which they are not equivalent, and provide a schedule for restoring the normal accident monitoring channels.

SURVEILLANCE REQUIREMENTS

A Note in the beginning of the SR table specifies that the following SRs apply to each AMI Function found in Table 3.3.11-1.

SR 3.3.11.1

Performance of the CHANNEL CHECK for each required instrument CHANNEL that is normally energized once every 31 days ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is a comparison of the parameter indicated on one CHANNEL to a similar parameter on other CHANNELS.

SURVEILLANCE REQUIREMENTS (continued)

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. 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 match criteria, it could be an indication that the sensor or the signal processing equipment has drifted outside its limit.

If the CHANNELS are within the match criteria, it is an indication that the CHANNELS are OPERABLE. If the CHANNELS are normally off scale during time when surveillance is required, the MEASUREMENT 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 given Function in any 31 day interval is a rare event. The MEASUREMENT CHANNEL CHECK supplements less formal, but more frequent, checks of CHANNEL OPERABILITY during normal operational use of the displays associated with this LCO's required CHANNELS.

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.11.2

A CHANNEL CALIBRATION is performed every 18 months. CHANNEL CALIBRATION is a complete check of the instrument CHANNEL including the sensor. The Surveillance verifies the CHANNEL responds to the measured parameter with the necessary range and accuracy.

For the Containment Upper Operating Area Radiation instrumentation, a CHANNEL CALIBRATION may consist of an electronic calibration of the CHANNEL, not including the detector, for range decades above 100 mSv/hr and one point calibration check of the detector below 100 mSv/hr with a gamma source.

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. DCD Tier 2, Chapter 7.
2. NRC RG 1.97, Rev.4, June 2006.
3. NUREG-0737, Supplement 1, January 1983.
4. IEEE Standard 603-1991.

B 3.3 INSTRUMENTATION

B 3.3.12 Remote Shutdown Display and Control

BASES

BACKGROUND

The remote shutdown display and control provides the main control room (MCR) operator with sufficient instrumentation and controls to place and maintain the unit in a safe shutdown condition from a location other than the MCR. This capability is necessary to protect against the possibility that the MCR becomes inaccessible. A safe shutdown condition is defined as MODE 3. With the unit in MODE 3, the auxiliary feedwater system (AFWS) 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 [AFWS] and the ability to borate the reactor coolant system (RCS) from outside the MCR allow extended operation in MODE 3.

In the event that the MCR becomes inaccessible, the operators can establish control at the remote shutdown console and place and maintain the unit in MODE 3. Not all controls and necessary transfer switches are located at the remote shutdown console. 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 console 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 MCR become inaccessible.

APPLICABLE SAFETY ANALYSES

The remote shutdown display and control is required to provide equipment at appropriate locations outside the MCR 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 display and control are located in 10 CFR 50, Appendix A, GDC 19 (Reference 1) and Appendix R (Reference 2).

The remote shutdown display and control satisfies Criterion 4 of 10 CFR 50.36(c)(2)(ii).

LCO

The remote shutdown display and control 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 MCR. The instrumentation and controls required are listed in Table 3.3.12-1.

The controls, instrumentation, and transfer switches are those required for:

a. Reactivity control (initial and long term)

b. RCS pressure control

c. Decay heat removal

d. RCS inventory control

e. Safety support systems for the above functions, as well as station service water, component cooling water, and onsite power

A Function of a remote shutdown display and control is OPERABLE if all instrument and control channels needed to support the remote shutdown Functions are OPERABLE. In some cases, Table 3.3.12-1 could indicate that the required information or control capability is available from several alternate sources. In these cases, the Remote Shutdown Console is OPERABLE as long as one channel of any of the alternate information or control sources for each Function is OPERABLE.

The remote shutdown display and control 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 Console be placed in operation.

APPLICABILITY

The remote shutdown display and control 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 MCR.

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 MCR instruments or control become unavailable.

ACTIONS

A Remote Shutdown Console division is inoperable when each function is not accomplished by at least one designated Remote Shutdown Console channel that satisfies the OPERABILITY criteria for the channel's function. These criteria are outlined in the LCO section of the Bases.

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 3.3.12-1. The Completion Time(s) of the inoperable channel(s)/division(s) of a Function will be tracked separated from the time the Condition was entered for that Function.

A.1

Condition A addresses the situation where one channels of the Remote Shutdown Console are inoperable. This includes the control and transfer switches for any required Function.

The Required Action is to restore the division to OPERABLE status within 31 days. The Completion Time is based on operating experience, and the low probability of an event that would require evacuation of the MCR.

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.

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 could 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 Console transfer switch and control circuit performs its intended function. This verification is performed from the remote shutdown console and locally, as appropriate. Operation of the equipment from the remote shutdown Console is not necessary. The Surveillance can be satisfied by performance of a continuity check. This will ensure that if the MCR 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 Console control channels seldom fail to pass the Surveillance when performed at a Frequency of once every 18 months.

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 in-place 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.

B 3.3 INSTRUMENTATION

B 3.3.13 Logarithmic Power Monitoring Channels

BASES

BACKGROUND

The logarithmic power monitoring channels provide neutron flux power indication from less than 10^{-7} % RTP to greater than 100 % RTP. They also provide reactor protection when the reactor trip switchgears (RTSGs) are shut, in the form of a Logarithmic Power Level – High trip.

This LCO addresses MODES 3, 4, and 5 with the RTSGs open. When the RTSGs are shut, the logarithmic power monitoring channels are addressed by LCO 3.3.2, "Reactor Protection System (RPS) Instrumentation – Shutdown."

When the RTSGs are open, two of the four logarithmic power monitoring 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 (logarithmic) power when the RTSGs 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. 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 one of 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. The logarithmic power monitoring channels 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 Reference 1. Reference 2 describes the specific logarithmic power monitoring channel features that are critical to comply with the GDC.

BASES

APPLICABLE SAFETY ANALYSES (continued)

The OPERABILITY of logarithmic power monitoring channels is necessary to meet the assumption of the safety analyses and to provide for the mitigation of accident and transient conditions.

The logarithmic power monitoring channels satisfy LCO SELECTION CRITERION 3.

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.

APPLICABILITY

In MODES 3, 4, and 5, with RTSGs 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 RTSGs 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 Protection System Instrumentation – Operating,” and LCO 3.3.2, “Reactor Protection System Instrumentation – Shutdown.”

The requirements for startup range neutron flux monitoring in MODE 6 are addressed in LCO 3.9.2, "Nuclear Instrumentaion" The startup range nuclear monitoring channels provide neutron flux coverage extending an additional one to two decades below the logarithmic channels for use during refueling, when neutron flux could be extremely low.

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.

A.1 and A.2

With one required channel inoperable, it may not be possible to perform a CHANNEL CHECK to verify that the other required channel is OPERABLE.

BASES

ACTIONS (continued)

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 therefore requires that all positive reactivity additions that are under operator control, such as boron dilution or reactor coolant system temperature changes, be halted immediately to preserve SDM.

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 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 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 the 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 indication, and readability. If a channel is outside of the criteria, it could be an indication that the preamplifier 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.

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, CHANNEL CHECK minimizes the chance of loss of protection function due to failure of redundant channels. CHANNEL CHECK supplements check of channel OPERABILITY during normal operational use of displays associated with the LCO required channels.

SR 3.3.13.2

A CHANNEL FUNCTIONAL TEST is performed every 31 days to ensure that the entire channel is capable of properly indicating neutron flux. Internal test circuitry is used to feed pre-adjusted 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:

The Setpoint Control Program (SCP) has controls which require verification that the instrument channel functions as required by verifying the as-left and as-found setting are consistent with those established by the setpoint methodology.

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 a remote display. 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 drifts between successive calibrations to ensure that the channel remains operational between successive surveillance. The SCP has controls which require verification that the instrument channel functions as required by verifying the as-left and as-found setting are consistent with those established by the setpoint methodology.

BASES

SURVEILLANCE REQUIREMENTS (continued)

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 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. DCD Tier 2, Section 7.1, 7.2, 7.5, 7.8, and 15.4.

B 3.3 INSTRUMENTATION

B 3.3.14 Boron Dilution Alarms

BASES

BACKGROUND

The boron dilution alarm system (BDAS) alerts the operator of a boron dilution event in MODES 3, 4 and 5. The boron dilution alarm is received at least 30 minutes prior to criticality in MODES 3, 4, and 5 to allow the operator to terminate the boron dilution.

In MODES 1 and 2, protection for a boron dilution event is presented in LCO 3.3.1, “Reactor Protection System (RPS) Instrumentation – Operating.” In MODES 3 and 4 with the CEAs withdrawn, LCO 3.3.2, “Reactor Protection System (RPS) Instrumentation – Shutdown,” provides protection. In MODE 6, protection for a boron dilution event is presented in LCO 3.9.2, “Nuclear Instrumentation.”

The boron dilution alarm system (BDAS) uses two channels that monitor the startup channel neutron flux indications. If the neutron flux signals increase to the calculated alarm setpoint an MCR annunciation is received. The setpoint is automatically lowered to a fixed amount above the current flux level signal. The alarm setpoint will only follow decreasing or constant flux levels, not increasing levels. Two channels of BDAS must be OPERABLE to provide single failure protection and to facilitate detection of channel failure by providing CHANNEL CHECK capability.

APPLICABLE SAFETY ANALYSES

The BDAS channels are necessary to monitor core reactivity changes. They are the primary means for detecting and triggering operator ACTIONS to respond to boron dilution events initiated from conditions in which the RPS is not required to be OPERABLE.

The OPERABILITY of BDAS channels is necessary to meet the assumptions of the safety analyses to mitigate the consequences of an inadvertent boron dilution event as described in the APR1400 DCD Tier 2, Chapter 15.

The BDAS channels satisfy LCO SELECTION CRITERION 3.

BASES

LCO

The LCO on the BDAS channels ensures that adequate information is available to mitigate the consequences of a boron dilution event.

At least two BDAS channels are required to be OPERABLE. Because the BDAS uses the excore startup channel instrumentation as its detection system, the OPERABILITY of the excore startup channel is also part of the OPERABILITY of the BDAS.

APPLICABILITY

The BDAS must be OPERABLE in MODES 3, 4, and 5 because the safety analysis assumes this alarm will be available in these MODES to alert the operator to take action to terminate the boron dilution. 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 Protection System (RPS) Instrumentation – Operating,” and LCO 3.3.2, “Reactor Protection System (RPS) Instrumentation – Shutdown.”

The requirements for source range neutron flux monitoring in MODE 6 are addressed in LCO 3.9.2, “Nuclear Instrumentation.” The excore startup channels provide neutron flux coverage extending an additional one to two decades below the logarithmic channels for use during shutdown and refueling when neutron flux could be extremely low.

The Applicability is modified by a Note that the BDAS is required in MODE 3 within 1 hour after the neutron flux is within the startup range following a reactor shutdown. This allows the neutron flux level to decay to a level within the range of the excore startup channels and for the operator to initialize the BDAS.

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.

Turn off charging pump immediately to prohibit a possible excessive positive reactivity addition if LCO 3.3.14 is not met. But, an auxiliary charging pump, which supplies a restricted charging flow, may be turned on if necessary.

ACTIONS (continued)

A.1 and A.2

With one required channel inoperable, Required Action A.1 requires the RCS boron concentration to be determined immediately and at the applicable monitoring Frequency specified in the COLR. The RCS boron concentration may be determined by the boronometer reading or by RCS sampling. The RCS sample should be from the hot leg if one or more reactor coolant pumps (RCPs) are running or from the discharge of the operating pump providing shutdown cooling flow with no RCPs running. The monitoring Frequency specified in the COLR ensures that a decrease in the boron concentration during a boron dilution event will be detected. The boron concentration measurement and the OPERABLE BDAS channel provide alternate methods of detection of boron dilution with sufficient time for termination of the event before the reactor achieves criticality.

According to Required Action A.2, the SDM is ensured, under the operator administrative control, by suspending all operations involving positive reactivity addition like the boron concentration or reactor coolant temperature change.

B.1 and B.2

With two required channels inoperable Required Action B.1 requires the RCS boron concentration to be determined by redundant methods immediately and at the monitoring Frequency specified in the COLR. The redundant methods may use the boronometer and RCS sampling or independent collection and analysis of two RCS samples. The RCS sample should be from the hot leg if one or more reactor coolant pumps (RCPs) are running or from the discharge of the operating pump providing shutdown cooling flow with no RCPs running. The simultaneous use of the boronometer and RCS sampling or independent collection and analysis of two RCS samples to monitor the RCS boron concentration provides alternate indications of inadvertent boron dilution. This will allow detection with sufficient time for termination of boron dilution before the reactor achieves criticality.

According to Required Action B.2, the SDM is ensured, under the operator administrative control, by suspending all operations involving positive reactivity addition like the boron concentration or reactor coolant temperature change.

SURVEILLANCE REQUIREMENTS

SR 3.3.14.1

SR 3.3.14.1 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 a 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. If a channel is outside of the criteria, it could 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.

This SR is modified by a Note that states the CHANNEL CHECK is not required to be performed until 1 hour after neutron flux is within the startup range.

SR 3.3.14.2

A CHANNEL FUNCTIONAL TEST is performed every 31 days of cumulative operation during shutdown to ensure that the BDAS is capable of properly alerting the operator to a boron dilution event.

SURVEILLANCE REQUIREMENTS (continued)

Internal excore startup channel test circuitry is used to feed pre-adjusted test signals into the excore startup channel to verify the proper neutron flux indication is received at the BDAS.

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 a change in channel output.

A CHANNEL FUNCTIONAL TEST of the BDAS consists of online tests including verification of the alarm in the MCR.

SR 3.3.14.3

SR 3.3.14.3 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 excore startup channel from the input through to the BDAS. 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. This SR is an extension of the SR 3.9.2.2 for the nuclear instrumentation CHANNEL CALIBRATION listed here because of its Applicability in MODES 3, 4 and 5.

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 a change in channel output.

REFERENCES

1. DCD Tier 2, Chapter 7.

2. DCD Tier 2, Chapter 15.

B 3.4 REACTOR COOLANT SYSTEM (RCS)

B 3.4.1 RCS Pressure, Temperature, and Flow Limits

BASES

BACKGROUND

These Bases address requirements for maintaining reactor coolant system (RCS) pressure, temperature, and flow rate within limits assumed in the safety analyses. The safety analyses (Reference 1) for normal operating conditions and anticipated operational occurrences (AOOs) assume initial conditions within the normal steady state envelope. The limits placed on DNB related parameters ensure that these parameters will not be less conservative than were assumed in the safety 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 the minimum and maximum PZR pressures are consistent with operation within the nominal operating envelope and are bounded by those used as the initial pressures in the safety 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 safety analyses.

The LCO limit for minimum RCS flow rate is bounded by the thermal design flow rate which is the minimum flow rate in the thermal analysis. 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 (Reference 1). The safety analyses have shown that transients initiated from the limits of this LCO will meet the DNBR criterion of greater than or equal to 1.29. 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 include loss of coolant flow events and dropped or stuck control element assembly (CEA) events.

BASES

APPLICABLE SAFETY ANALYSES (continued)

A key assumption for the analysis of these events is that the core power distribution is within the limits of LCO 3.1.7, "Regulating Control Element Assembly (CEA) Insertion Limits," LCO 3.1.8, "Part Strength Control Element Assembly (CEA) Insertion Limits," LCO 3.2.3, “AZIMUTHAL POWER TILT (T_q),” and LCO 3.2.5, “AXIAL SHAPE INDEX (ASI).” The safety analyses are performed over the following range of initial values: RCS pressure 151.9 to 162.4 kg/cm^{2}G (2,160 to 2,310 psig), core inlet temperature greater than or equal to 285 °C (545 °F) and less than or equal to 295 °C(563°F) for less than 90 % of RTP, or greater than or equal to 287.8 °C (550°F) and less than or equal to 295 °C (563°F) for greater than or equal to 90 % of RTP, and reactor vessel inlet coolant flow rate 95 to 116 %.

The RCS DNB limits satisfy LCO SELECTION CRITERION 2.

LCO

This LCO specifies limits on the monitored process variables: 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 value for flow rate has 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 for RCS flow rate, MODES 1 and 2 for RCS pressurizer pressure, MODE 1 for RCS cold leg temperature, and MODE 2 with k_{eff} greater than or equal to 1.0 for RCS cold leg temperature, the limits 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.

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 could have been exceeded.

BASES

ACTIONS

A.1

RCS total flow rate is not a controllable parameter and is not expected to vary during steady state operation. If the flow rate is not within the LCO limit, action must be taken to restore DNB margin.

The 2-hour Completion Time for restoration of RCS flow rate provides sufficient time 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.

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 MODE 2 in 6 hours. In MODE 2, the reduced power condition eliminates the potential for violation of the accident analysis bounds.

The 6 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 heat removal.

C.1

Pressurizer pressure and RCS cold leg temperature is a controllable and measurable parameters. 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, the plant must be brought to MODE 3. In MODE 3, the potential for violation of the DNB limits is greatly reduced.

The 6-hour Completion Time is a reasonable time that permits the plant power to be reduced at an orderly rate in conjunction with even control of steam generator heat removal.

SURVEILLANCE REQUIREMENTS

SR 3.4.1.1

This SR ensures that pressurizer pressure is within limit. The 12-hour Frequency has been shown by operating practice to be sufficient to regularly assess degradation and verify operation within safety analysis assumptions.

SR 3.4.1.2

This SR ensures that RCS cold leg temperature is within limit. The 12-hour Frequency has been shown by operating practice to be sufficient to regularly assess for potential degradation and to verify operation is within safety analysis assumptions.

Since the measurement uncertainty for RCS cold leg temperature of data processing system is lower than that of indicator, whether or not the violation of the LCO shall be verified using the RCS cold leg temperature of data processing system, if the RCS cold leg temperature is accessing the LCO.

SR 3.4.1.3

This SR 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 potential degradation and to verify operation is within thermal analysis assumptions.

The measurement uncertainty shall be incorporated into the measured RCS flow rate for performing this Surveillance.

SR 3.4.1.4

The RCS total flow rate is measured by performance of a precision calorimetric heat balance once per 31 days. This verifies that the actual RCS total flow rate is within the bounds of the analyses.

Because the RCS flow rate is not excepted to vary during plant operation, the 31-day Surveillance Frequency is sufficient to verify the RCS total flow rate is within the range of design.

The measurement uncertainty shall be incorporated into measured RCS total flow rate for performing this Surveillance.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The SR is modified by a Note which states the SR is only required to be performed 24 hours after reaching 95 % RTP. The SR cannot be performed in MODE 2 or below and will not yield accurate results if performed below 95 % RTP.

REFERENCES

1. DCD Tier 2, Chapter 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

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 285 to 295 °C (545 to 563 °F). Nominal temperature T_{cold} for making the reactor critical is 290.6 °C (555 °F). Safety and operating analyses for lower temperatures have not been completed.

APPLICABLE SAFETY ANALYSES

There are no accident analyses which dictate the minimum temperature for criticality, but all low power safety analyses (Reference 1) assume initial temperatures near the 286.7 °C (548 °F) limit. The temperature is a value which is added the lower limit of cold leg temperature, that is, the safety analysis initial condition of 285 °C (545 °F) to 1.7 °C (3 °F) of uncertainty.

The RCS minimum temperature for criticality satisfies LCO SELECTION CRITERION 2.

LCO

The purpose of the LCO is to prevent criticality below the minimum normal operating temperature and to prevent operation in an unanalyzed regime.

The LCO is only applicable below 289.4 °C (553 °F) and provides a reasonable distance to the limit of 286.7 °C (548 °F). This allows adequate time to trend its approach and take corrective actions prior to exceeding the limit.

BASES

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 MODES 1 and 2 when k_{eff} greater than or equal to 1.0. Monitoring for RCS temperature is required at or below a T_{cold} of 289.4 °C (553 °F). The no-load temperature of 291.3 °C (556.3 °F) is maintained by the steam bypass system.

ACTIONS

A.1

If T_{cold} is below 286.7 °C (548 °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 3 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 maintain the plant within the analyzed range.

SURVEILLANCE REQUIREMENTS

SR 3.4.2.1

First Frequency requires T_{cold} to be verified greater than or equal to 286.7 °C (548 °F) within 15 minutes prior to achieving criticality. The 15-minute time period allows the operator to adjust temperatures or delay criticality so the LCO will not be violated. A Note of second Frequency states this Surveillance is required whenever the reactor is critical and T_{cold} is below 289.4 °C (553 °F). In this case, T_{cold} is required to be verified at or above 286.7 °C (548 °F) every 30 minutes. The 30-minute time is Frequency enough to prevent inadvertent violation of the LCO.

Since the measurement uncertainty for RCS cold leg temperature of Data Processing System is lower than that of indicator, whether or not the violation of the LCO shall be verified using the RCS cold leg temperature of Data Processing System, if the RCS cold leg temperature is approaching to the LCO.

REFERENCES

1. DCD Tier 2, Chapter 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 (Reference 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 curves 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 reactor vessel is the component most subject to brittle failure, and the LCO limits apply mainly to the reactor vessel. The limits do not apply to the pressurizer, which has different design characteristics and operating functions.

10 CFR 50, Appendix G (Reference 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 American Society of Mechanical Engineers (ASME) Code, Section XI, Appendix G (Reference 3).

BACKGROUND (continued)

The actual shift in the RT_{NDT} of the reactor vessel material will be established periodically by removing and evaluating the irradiated reactor vessel material specimens, in accordance with ASTM E 185 (Reference 4) and Appendix H of 10 CFR 50 (Reference 5). The operating P/T limit curves will be adjusted, as necessary, based on the evaluation findings and the recommendations of Reference 3.

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 reactor vessel wall are reversed. The thermal gradient reversal alters the location of the tensile stress from the outer to inner walls.

The criticality limit includes the Reference 2 requirement that the limit be no less than 22 °C (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 non-isolable 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 (Reference 6), provides a recommended methodology for evaluating an operating event that causes an excursion outside the limits.

BASES

APPLICABLE SAFETY ANALYSES

The P/T limits are not derived from design basis event (DBE). They are prescribed during normal operation to avoid encountering pressure, temperature, and temperature rate of change conditions that may cause undetected flaws to propagate and cause non-ductile failure of the RCPB, an unanalyzed condition. Since the P/T limits are not derived from any DBE, there are no acceptance limits related to the P/T curves. Rather, the P/T curves are acceptance limits themselves since they preclude operation in an unanalyzed condition.

The RCS P/T limits satisfy LCO SELECTION CRITERION 2.

LCO

The two elements of this LCO are:

a. The limit curves for heatup, cooldown, and ISLH testing

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 non-ductile failure.

The limits for rate-of-change of temperature control the thermal gradient through the walls and is used as input 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.

Violation of the LCO limits places the reactor vessel outside of the bounds of the stress analysis and can increase stresses in other RCPB components. The consequences depend on several factors, as follows:

a. The severity of the departure from the operating P/T regime or the severity of the rate-of-change of temperature

b. The length of time that the limits were violated (longer violations allow the temperature gradient in the thick walls of the vessel to become more pronounced)

c. The existences, sizes, and orientations of flaws in the vessel material

BASES

APPLICABILITY

The RCS P/T limits provides a definition of acceptable operation for prevention of non-ductile failure that is in accordance with 10 CFR 50, Appendix G (Reference 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 non-ductile failure. At all times is defined to be any condition with fuel in the reactor vessel. The limits do not apply to the pressurizer.

During MODES 1 and 2, other Technical Specifications (TS) 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 Limits,” LCO 3.4.2, “RCS Minimum Temperature for Criticality,” and SL 2.1, “Safety Limits” also provides operational restrictions for pressure and temperature and maximum pressure.

Furthermore, MODES 1 and 2 are above the temperature range of concern for non-ductile 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. A violation of P/T limits caused by abnormal transients, which could be accompanied by equipment failures, may also require additional ACTIONS based on emergency operating procedures.

Since the RCS cannot be pressurized with the reactor vessel closure head detensioned, the limits of pressure, temperature, and rate of heatup and cooldown do not be applied.

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 analysis.

The Completion Time of 30 minutes 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.

ACTIONS (continued)

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 analysis, new analyses, or inspection of the components.

ASME Code, Section XI, Appendix E (Reference 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 a reasonable time 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 could have occurred and could have affected the RCPB integrity.

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.

b. A sufficiently severe event caused entry into an unacceptable region.

Either possibility indicates a need for more careful examination of the event, which is best accomplished with the RCS at reduced pressure and temperature state. With reduced pressure and temperature conditions, the possibility of propagation of undetected flaws is decreased.

ACTIONS (continued)

Pressure and temperature are reduced by placing the plant in MODE 3 within 6 hours and in MODE 5 with RCS pressure less than 33.7 kg/cm^{2}A (479 psia) 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.

C1. 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.

ASME Code, Section XI, Appendix E (Reference 6), may be used to support the evaluation. However, its use is restricted to evaluation of the reactor vessel beltline.

The Completion Time 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.

BASES

ACTIONS (continued)

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 could have occurred and could 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 temperature and pressure conditions are undergoing planned changes. This Frequency is considered reasonable in view of the MCR indication available to monitor RCS status. Also, since temperature rate-of-change limits are specified in hourly increments, 30-minute periods permit assessment and correction for minor deviations within a reasonable time.

Surveillance for heatup, cooldown, or ISLH testing may be discontinued when definitions given in the plant procedures for ending the activity is satisfied.

The SR is modified by a Note which states that this SR be performed only during RCS system heatup, cooldown, and ISLH testing. There are no Surveillance Requirements during critical operation because LCO 3.4.2, contains a more restrictive requirement.

REFERENCES

1. APR1400-Z-M-NR-13010-P, “Pressure-Temperature Limits Methodology for RCS Heatup and Cooldown Technical Report.”, September 2013.

2. 10 CFR 50, Appendix G.

3. ASME Section XI, Appendix G.

4. ASTM E 185, July 1988.

5. 10 CFR 50, Appendix H.

6. ASME 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

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 (Reference 1). 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 event (DBE) 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.

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 is 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, and single pump broken shaft or coastdown, and rod withdrawal events (Reference 1).

For four pump operation, the transient state DNB analysis, which generates the pressure and temperature and Safety Limit (i.e., the departure from nucleate boiling ratio (DNBR) limit), had been performed for a maximum THERMAL POWER level. The accident analysis setpoint of the nuclear overpower (high flux) trip is based on an analysis assumption that bounds possible instrumentation errors. The DNBR limit is established statistically combining the system design values with the critical heat flux correlation limit.

RCS Loops – MODES 1 and 2 satisfy LCO SELECTION CRITERIA 2 and 3.

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 steam generators. To meet safety analysis acceptance criteria for DNB, four pumps are required in MODES 1 and 2.

Each OPERABLE loop consists of two RCPs providing forced flow for heat transport to a steam generator which is OPERABLE in accordance with the steam generator tube surveillance program. Steam generator, 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 less than or equal to 45.0 % wide range as sensed by the RPS. The minimum water level to declare the SG OPERABLE is 25 % WR.

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 System (SCS) and Coolant Circulation – High Water Level”, and

LCO 3.9.5, “Shutdown Cooling System (SCS) and Coolant Circulation – Low Water Level”

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 a reasonable, based on operating experience, to reach MODE 3 from full power conditions in an orderly manner and without challenging safety systems.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.4.4.1

This SR requires verification every 12 hours of the required number of RCS 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 analysis assumptions. In addition, MCR indication and alarm will normally indicate loop status.

REFERENCES

1. DCD Tier 2, Chapter 15.

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 running is sufficient to remove core decay heat. However, two RCS loops are required to be OPERABLE to satisfy single failure criteria. Only one RCP need 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 can result in challenges to a fission product barrier. The RCS loops are part of the primary success path which functions or actuates to prevent or mitigate a design basis event (DBE) 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 LCO SELECTION CRITERION 3.

BASES

LCO

The purpose of this LCO is to require two RCS loops to be available for heat removal, thus providing redundancy. The LCO requires the two RCS loops to be OPERABLE with the intent of requiring both SGs to be capable (greater than or equal to 25 % WR 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.

The Note permits a limited period of operation without RCPs. All RCPs may be de-energized for less than or equal to 1 hour per 8-hour period. This means that natural circulation has been established. When in natural circulation, boron reduction is prohibited because an even concentration distribution throughout the RCS cannot be ensured. Core outlet temperature is to be maintained at least 5.6 °C (10 °F) below the saturation temperature so that no vapor bubble could 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 (SC) pump forced circulation (e.g., to change operation from one SC train to the other, to perform surveillance or startup testing, to perform the transition to and from SC System cooling, or to avoid operation below the RCP minimum NPSH 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 in accordance with the steam generator tube surveillance program. An 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”

BASES

APPLICABILITY (continued)

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 System (SCS) and Coolant Circulation – High Water Level”, and

LCO 3.9.5, “Shutdown Cooling System (SCS) and Coolant Circulation – Low Water Level”

ACTIONS

A.1

If one RCS loop is inoperable, redundancy for forced flow heat removal is lost. The Required Action is restoration of the required RCS loop to OPERABLE status within a Completion Time of 72 hours. This time allowance is a justified period to be without the redundant, non-operating loop because a single loop in operation has a heat transfer capability much 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 shutdown cooling system. The Completion Time of 12 hours is compatible with required operation to achieve cooldowns and depressurization from the existing plant condition in an orderly manner and without challenging plant systems.

C.1 and C.2

If no RCS loop is OPERABLE or in operation, except as provided by the Note in the LCO section, all operations involving a reduction of RCS boron concentration must be immediately suspended. This is necessary because boron dilution requires forced circulation for proper homogenization. Action to restore one RCS loop to OPERABLE status and operation shall be immediately initiated and continued until one RCS loop is restored to OPERABLE status and operation. The immediate Completion Times reflect the importance of maintaining operation for decay heat removal.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.4.5.1

This SR requires verification every 12 hours that the required number of RCS loops are operation. Verification includes flow rate, temperature, and pump status monitoring, which help ensure that forced flow is providing heat removal. The 12-hour Frequency has been shown by operating practice to be sufficient to regularly assess degradation and verify operation within safety analysis assumptions. In addition, MCR indication and alarm will normally indicate loop status.

SR 3.4.5.2

This SR requires verification every 12 hours that the secondary side water level in each SG is greater than or equal to 25 % wide range. 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 Frequency has been shown by operating practice to be sufficient to regularly assess degradation and verify operation within the safety analysis assumptions.

SR 3.4.5.3

Verification that the required number of RCPs are 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 the required RCPs. The 7-day Frequency is considered reasonable in view of other administrative controls available and has been shown to be acceptable by operating experience.

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 (SC) 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 SC trains can be used for coolant circulation. The intent of this LCO is to provide forced flow from at least one RCP or one SC train for decay heat removal and transport. The flow provided by one RCP or SC 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 SC trains provide this circulation.

RCS Loops – MODE 4 have been included in Specification as important contributors to risk reduction according to LCO SELECTION CRITERION 4.

LCO

The purpose of this LCO is to require that at least two RCS loops or SC trains shall 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 loops and SC trains. 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 SC pumps to be de-energized less than or equal to 1 hour per 8-hour period. This means that natural circulation has been established using the steam generators. The Note 1 prohibits boron dilution when forced flow is stopped because an even concentration distribution cannot be ensured.

LCO (continued)

Core outlet temperature is to be maintained at least 5.6 °C (10 °F) below saturation temperature so that no vapor bubble can form and possibly cause a natural circulation flow obstruction. The response of the RCS without the RCPs or SC pumps depends on the core decay heat load and the length of time that the 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 SC flow or heat removal via the SGs must be re-established prior to reaching the pressure limit. The circumstances for stopping both RCPs or SC 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 5.6 °C (10 °F) subcooling limits.

b. An alternate heat removal path through the SGs is in operation.

Note 2 requires, before an RCP is started with any RCS cold leg temperature less than or equal to less than or equal to the LTOP enable temperature specified in the PTLR, that secondary side water temperature in each SG is less than 55.6 °C (100 °F) above each of the RCS cold leg temperatures.

Satisfying 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 in accordance with the steam generator tube surveillance program and has the minimum water level specified in SR 3.4.6.2.

Similarly, for the SC system, an OPERABLE SC train is composed of the OPERABLE SC pump capable of providing forced flow to the SC heat exchanger.

RCPs and SC 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 SC 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 System (SCS) and Coolant Circulation – High Water Level”, and

LCO 3.9.5, “Shutdown Cooling System (SCS) and Coolant Circulation – Low Water Level”

ACTIONS

A.1

If only one required RCS loop is OPERABLE and in operation and no SC trains are OPERABLE, redundancy for heat removal is lost. The Required Action must be initiated immediately to restore a second RCS loop or SC train to OPERABLE status.

The immediate Completion Time reflects the importance of maintaining the availability of two paths for heat removal.

B.1

If only one required SC train is OPERABLE and in operation and no RCS loops are OPERABLE, redundancy for heat removal is lost. 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 SC train OPERABLE, redundancy for decay heat removal is lost and, in the event of a loss of the remaining SC train, it would be safer to initiate that loss from MODE 5 (less than or equal to 98.9 ^{o}C [210 °F]) rather than MODE 4 (98.9 ^{o}C – 176.7 ^{o}C [210 °F – 350 °F]). The Completion Time of 24 hours is reasonable based on operating experience to reach MODE 5 from MODE 4, with only one SC train operating, in an orderly manner and without challenging plant systems.

BASES

ACTIONS (continued)

C.1 and C.2

If no RCS loops or SC train are OPERABLE or in operation, except during conditions permitted by Note 1 in the LCO section, all operations involving reduction of RCS boron concentration must be suspended and action to restore one RCS loop or SC train to OPERABLE status and operation must be initiated. Boron dilution requires forced circulation for proper mixing, and the margin to criticality must not be reduced in this type of operation. The immediate Completion Time reflects the importance of maintaining operation for decay heat removal. The action to restore must be continued until one loop or train is restored to operation.

SURVEILLANCE REQUIREMENTS

SR 3.4.6.1

This SR requires verification every 12 hours that one required loop or train is in operation. This ensures forced flow is providing heat removal. Verification includes flow rate, temperature, and pump status monitoring. The 12-hour Frequency has been shown by operating practice to be sufficient to regularly assess RCS loop status.

In addition, MCR indication and alarms will normally indicate status.

SR 3.4.6.2

This SR requires verification every 12 hours of secondary side water level in the required steam generator(s) greater than or equal to 25 % WR. 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 Frequency has been shown by operating practice to be sufficient to regularly assess degradation and verify operation within safety analyses assumptions.

SR 3.4.6.3

Verification that the required pump OPERABLE ensures that an additional RCS loop or SC train can be placed in operation, if needed to maintain decay heat removal and reactor coolant circulation.

BASES

SURVEILLANCE REQUIREMENTS (continued)

Verification is performed by verifying proper breaker alignment and power available to the required pumps. The 7-day Frequency is considered reasonable in view of other administrative controls available and has been shown to be acceptable by operating experience.

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 generators (SGs) secondary side coolant or the component cooling water via shutdown cooling (SC) heat exchangers. While the principal means for decay heat removal is via the SC system, the SGs 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 SC 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 SC train for decay heat removal and transport. The flow provided by one SC 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 SC train that must be OPERABLE and in operation. The second path can be another OPERABLE SC train, or through the SGs, 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 SC trains provide this circulation.

RCS loops – MODE 5 (loops filled) have been included in Specification as important contributors to risk reduction according to LCO SELECTION CRITERION 4.

LCO

The purpose of this LCO is to require at least one of the SC trains be OPERABLE and in operation with an additional SC train OPERABLE or secondary side water level of each SG shall be greater than or equal to 25 % wide range. One SC train provides sufficient forced circulation to perform the safety functions of the reactor coolant under these conditions. The second SC train is normally maintained OPERABLE as a backup to the operating SC train to provide redundant paths for decay heat removal. However, if the standby SC trains is not OPERABLE, a sufficient alternate method to provide redundant paths for decay heat removal is two SGs with their secondary side water levels greater than or equal to 25 % wide range. Should the operating SC train fail, the SGs could be used to remove the decay heat.

Note 1 permits all SC pumps to be de-energized less than or equal to 1 hour per 8-hour period. The circumstances for stopping both SC trains are to be limited to situations where pressure and temperature increases can be maintained well within the allowable pressure (pressure and temperature [P/T] limits or low temperature overpressure protection [LTOP] limits) and 5.6 °C (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 when SC forced flow is stopped because an even concentration distribution cannot be ensured. Core outlet temperature is to be maintained at least 5.6 °C (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 SC 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 RCPs or SC forced circulation. This is permitted to change operation from one SC train to the other, perform surveillance or startup testing, perform the transition to and from the SC system, 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.

BASES

LCO (continued)

Note 2 allows one SC train to be inoperable for a period of up to 2 hours provided that the other SC 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.

Note 3 requires that before an RCP may be started with any RCS cold leg temperature less than or equal to less than or equal to the LTOP enable temperature specified in the PTLR, that secondary side water temperature in each SG is less than 55.6 °C (100 °F) above each of the RCS cold leg temperatures.

Satisfying 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 removal of SC trains from 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 SC trains.

An OPERABLE SC train is composed of an OPERABLE SC pump and an OPERABLE SC heat exchanger.

SC pumps are OPERABLE if they are capable of being powered and are able to provide flow if required. An OPERABLE SG can perform as a heat sink when it has an adequate secondary water level and is OPERABLE in accordance with the In-service Inspection Program.

Note 5 permits the alignment of a containment spray pump if a SC pump is not available or becomes inoperable. These pumps are designed to be interchangeable for operational flexibility.

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 SC train provides sufficient circulation for these purposes.

BASES

APPLICABILITY (continued)

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 System (SCS) and Coolant Circulation – High Water Level”, and

LCO 3.9.5, “Shutdown Cooling System (SCS) and Coolant Circulation – Low Water Level"

ACTIONS

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

If the required SC train is inoperable and any SGs have secondary side water levels less than 25 % wide range, redundancy for heat removal is lost. Action must be initiated immediately to restore a second SC train to OPERABLE status or to restore the water level in the required SGs. Either Required Action A.1 or Required Action A.1 and A.2 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 both SC trains are inoperable or no SC train is in operation, except as permitted in Note 1, all operations involving the reduction of RCS boron concentration must be suspended. Action to restore one SC train to OPERABLE status and operation must be initiated immediately. Boron dilution requires forced circulation for proper mixing and margin to criticality must not be reduced in this type of operation. The immediate Completion Times reflect the importance of maintaining operation for decay heat removal.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.4.7.1

This SR requires verification every 12 hours that one SC 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, MCR indication and alarms will normally indicate loop status.

The SC flow is established to ensure that core outlet temperature is maintained sufficiently below saturation to allow time for swap over to the standby SC train should the operating train be lost.

SR 3.4.7.2

Verifying the SGs are OPERABLE by ensuring their secondary side water levels are greater than or equal to 25 % wide range ensures that redundant heat removal paths are available if the second SC train is inoperable.

The Surveillance is required to be performed when the LCO requirement is being met by use of the SGs. If both SC 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 the second SC 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 the required pump. The Surveillance is required to be performed when the LCO requirement is being met by one of two SC trains (e.g., SGs have less than 25 % wide range water level). The 7-day Frequency is considered reasonable in view of other administrative controls available and has been shown to be acceptable by operating experience.

REFERENCES None.

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 reactor coolant system (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 (SC) heat exchangers. The steam generators 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 soluble neutron poison, boric acid.

In MODE 5 with loops not filled, only the SC 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 SC train for decay heat removal and transport. The other intent of this LCO is to require that two paths be available to provide redundancy for heat removal.

This LCO permits limited periods without forced circulation. When the SC trains are not in operation, no alternate heat removal path exists. The response of the RCS without the SC system depends on the decay heat load and the length of time that the SC pumps are stopped. As decay heat diminishes, the effects on RCS temperature diminish. Without cooling by SC system, higher heat loads will cause the reactor coolant temperature to increase at a rate proportional to the decay heat load. Because pressure can increase, applicable system pressure limits (pressure and temperature limits or low temperature overpressurization limits) must be observed and forced SC system flow must be reestablished prior to reaching the pressure limit. Entry into a condition with no SC system train in operation stops heat removal and should only be considered for limited circumstances such as when switching from one SC system train to the other. With the SC pumps stopped, pressure and temperature could increase and pumps must be restored prior to exceeding pressure and subcooling limits.

The SC system removes decay heat from the RCS and transfers the heat to the component cooling water (CCW) system. During “Loops Not Filled” operations the interruption or loss of SCS flow, decay heat removal (DHR) capability, can lead to bulk boiling quite rapidly.

BASES

BACKGROUND (continued)

In some cases, this can occur in 15 to 20 minutes. During “Loops Not Filled” operations, the SC system is the primary means of decay 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 SC trains provide this circulation. The flow provided by one SC train is adequate for decay heat removal and for boron mixing.

RCS loops – MODE 5 (loops not filled) has been included in specification as important contributors to risk reduction according to LCO SELECTION CRITERION 4.

LCO

The purpose of this LCO is to require a minimum of two SC trains be OPERABLE and one of these trains be in operation. An OPERABLE train is one that has the capability of transferring heat from the reactor coolant at a controlled rate.

Heat removal cannot occur via the SC system unless forced flow is used. A minimum of one running SC pump meets the LCO requirement for one train in operation. An additional SC train is required to be OPERABLE to meet the single failure criterion.

During Loops Not Filled operations, the containment spray pump in the OPERABLE SC train shall be OPERABLE.

Note 1 permits the SC pumps to be de-energized for less than or equal to 15 minutes when switching from one train to another. The circumstances for stopping both SC pumps are to be limited to situations when the outage time is short and the core outlet temperature is maintained at least 5.6 °C (10°F) below saturation temperature. The Note prohibits boron dilution and draining operations when SC forced flow is stopped.

Note 2 allows one SC 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 SC train is composed of an OPERABLE SC pump capable of providing forced flow to an OPERABLE SC heat exchanger, along with the appropriate flow and temperature instrumentation for control, protection, and indication. SC pumps are OPERABLE if they are capable of being powered and are able to provide flow if required.

Note 3 permits the alignment of a containment spray pump if an SC pump is not available or becomes inoperable. These pumps are designed to be interchangeable for operational flexibility.

APPLICABILITY

In MODE 5 with loops not filled, this LCO requires core heat removal and coolant circulation by the SCS.

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 System (SCS) and Coolant Circulation – High Water Level”, and

LCO 3.9.5, “Shutdown Cooling System (SCS) and Coolant Circulation – Low Water Level”

ACTIONS

A.1

If one required SC train is inoperable, redundancy for heat removal is lost. Action must be initiated immediately to restore a second train to OPERABLE status. The immediate Completion Time reflects the importance of maintaining the availability of two paths for heat removal.

BASES

ACTIONS (continued)

B.1, B.2 and B.3

If required SC trains are inoperable or no train is in operation, the action requires immediate suspension of any operation for boron concentration reduction, initiating action to raise RCS level to greater than EL 38.72 m (127 ft 1/4 in) and requires action to immediately start restoration of one SC train to OPERABLE status. Boron dilution requires forced circulation for proper mixing and margin to criticality must not be reduced in this type of operation. The immediate Completion Time reflects the importance of maintaining operation for decay heat removal.

SURVEILLANCE REQUIREMENTS

SR 3.4.8.1

This SR requires verification of the required SC train is in operation every 12 hours.

Verification includes flow rate, temperature, or pump status monitoring, which help ensure 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 within safety analyses assumptions.

SR 3.4.8.2

Verification that the required number of trains are OPERABLE ensures that redundant paths for heat removal are available and additional trains 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 the required pumps.

The 7-day Frequency is considered reasonable in view of other administrative controls available and has been shown to be acceptable by operating experience.

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 proportional heaters and their backup heater controls, and emergency power supplies. POSRVs are addressed by LCO 3.4.10, “Pressurizer Pilot Operated Safety Relief Valves.”

The maximum steady state water level limit in the pressurizer has been established to ensure that a liquid-to-vapor interface exists to permit RCS pressure control, using sprays and heaters during normal operation and proper pressure response for anticipated design basis transients (Reference 2). The maximum and minimum steady state 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.

b. By restricting the level to a maximum, expected transient reactor coolant volume increases (pressurizer insurge) will not cause excessive level changes which could result in degraded ability for pressure control.

The maximum steady state water level limit in the pressurizer 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 (POSRVs) can control pressure by steam relief rather than water relief (Reference 2). 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 may exceed the safety limit of 193.3 kg/cm^{2}A (2,750 psia).

BACKGROUND (continued)

The minimum steady state water level in the pressurizer assures pressurizer heaters, which are required to achieve and maintain pressure control, remain covered with water to prevent failure, which could occur if the heaters were energized uncovered.

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 a loss of single phase flow and a 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 non-condensible gases normally present.

Safety analyses presented in DCD Tier 2 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 credited in accident analysis, the need to maintain subcooling in the long term during loss of offsite power, as indicated in NUREG-0737 (Reference 1), is the reason for inclusion. The requirement for emergency power supplies is based on NUREG-0737 (Reference 1). The intent is to allow maintaining 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 with turbine trip assumed in many accident analyses, maintaining hot, high pressure conditions over an extended time period is not evaluated as part of the accident analyses.

The pressurizer satisfies the LCO SELECTION CRITERIA 2 and 3.

BASES

LCO

The LCO requirement for the pressurizer to be OPERABLE with water level greater than or equal to 25 % and less than or equal to 56 % ensures that a steam bubble exists. Limiting the maximum operating water level preserves the steam for pressure control. The minimum operating water level is established pressurizer heaters remain covered with water to prevent failure, which could occur if the heaters were energized uncovered in steam bubble region. The intent of the LCO is to ensure that a steam bubble exists in the pressurizer to minimize the consequences of potential overpressure transients.

The LCO requires two groups of OPERABLE pressurizer heaters, each with a capacity greater than or equal to 300 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 300 kW is derived from the use of 6 heaters rated at 50 kW each. The amount needed to maintain pressure is dependent on the ambient heat losses.

APPLICABILITY

The need for pressurizer 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, 2, and 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 3.4.11, “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 supplies. In the event of a loss of offsite power, the initial conditions of these MODES give 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, B.1 and B.2

With pressurizer water level outside the limits, action must be taken within 1 hour to restore the plant to operation within the bounds of the safety analyses. If pressurizer water level cannot be restored to within the limits in 1 hour, this is done by placing the plant in MODE 3 with the reactor trip switch gears open within 6 hours, and placing the plant in 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.

The Completion Time of 6 hours is a reasonable time 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 into a MODE where the LCO is not applicable. The 12-hour time to reach the non-applicable MODE is reasonable based on operating experience for that evaluation.

C.1

If one required group of pressurizer heaters is inoperable, restoration is required in 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. RCS pressure control may be maintained during this time using normal station powered heaters.

D.1 and D.2

If one required group of pressurizer heaters is inoperable and cannot be restored within the allowed Completion Time of Required Action C.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 SR 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 and above the nominal lower limit to prevent failure, which could occur if the heaters were energized uncovered. The Surveillance is performed by observing indicated level.

The 12-hour interval has been shown by operating practice to be sufficient to regularly assess degradation and verify operation within safety analysis assumptions. Alarms are also available for early detection of abnormal level indications.

SR 3.4.9.2

The SR 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 92-day Frequency is considered adequate to detect heater degradation and has been shown by operating experience to be acceptable.

SR 3.4.9.3

This SR 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, II.E.3.1, November 1980.

2. DCD Tier 2, Chaper 15.

B 3.4 REACTOR COOLANT SYSTEM (RCS)

B 3.4.10 Pressurizer Pilot Operated Safety Relief Valves (POSRVs)

BASES

BACKGROUND

Pressurizer POSRVs are designed to provide overpressure protection function and rapid depressurization function for reactor coolant system (RCS). Two spring-loaded pilot valves per each main valve are installed to provide RCS overpressure protection. Motor operated isolation valves and manual isolation valves are installed to isolate spring-loaded pilot valves, which are maintained open position during normal operation. Two motor operated pilot valves per each main valve are installed in series to provide rapid depressurization function. These motor operated pilot valves are maintained closed position during normal operation. Operating in conjunction with the reactor protection system, four valves are used to ensure that the safety limit (SL) of 193.3 kg/cm^{2}A (2,750 psia) is not exceeded for analyzed transients during operation in MODES 1 and 2. Four POSRVs are always used for MODE 3 and a portion of MODE 4. For the remainder of MODE 4 and for MODE 5, overpressure protection is provided by operating procedures and LCO 3.4.11.

The self-actuated pressurizer POSRVs are designed in accordance with the requirements set forth in the ASME Boiler and Pressure Vessel Code, Section III (Reference 1). The pressurizer POSRVs discharge steam from the pressurizer to the in-containment refueling water storage tank (IRWST) located in the containment.

The lift pressure setpoint for four pressurizer POSRVs is 173.7 kg/cm^{2}A (2,470 psia). The lift pressure for four POSRVs is established to prevent the RCS pressure from exceeding SL and maintain the assumed conditions of analyses. For testing the lift pressure setpoint, the upper and lower lift pressure limits for verified allowable range (As-Found Setpoint) of ±1.5 % are established based on 0.5 % of the measurement uncertainty of examination equipment plus some operating margin. After testing, however, the allowable range of setpoint (As-Left Setpoint) is adjusted within the ±0.75 % being considered by the change of lift setting and operating margin according to operating environmental factors. The lift setting is for the ambient conditions associated with MODES 1, 2, and 3. This requires that the valves be set a hot condition.

BACKGROUND (continued)

The overpressure protection function of the POSRVs is achieved by opening the main valve according to opening the spring-loaded pilot valves, resulting in a pressure discharge function. Time difference exists between the opening of pilot valves and the opening of main valves according to their dead time and actuation time, caused by the characteristics of POSRVs. The required opening time of the valve is limited to within 0.5 seconds.

Therefore, it is OPERABLE status if the lift setting of two spring-loaded pilot valves per valve satisfies the above requirements and the requirement of opening time for main valve. Since safety analyses do not take credit for motor operated isolation valve operation to mitigate the transition status according to inadvertent opening of spring-loaded pilot valves, this function is not categorized to safety function.

The pressurizer POSRVs are parts of the primary success paths and mitigate the effects of postulated accidents. OPERABILITY of the POSRVs ensures that the RCS pressure will be limited to 110 % of design pressure. The consequences of exceeding the ASME pressure limit (Reference 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 safety analyses in DCD Tier 2 which require safety valve actuation assume operation of all POSRVs to limit increasing RCS pressure. The opening time of valve uses 0.55 seconds and the nominal lift setting of POSRV includes the uncertainty of ± 2 %. In total uncertainties, the uncertainty of instrumentation equipment includes 0.5 % to verify the lift setting of pressurizer POSRVs.

These valves must accommodate pressurizer insurges, which could occur during various heatup events such as rod withdrawal, ejected rod, loss of main feedwater, loss of load or main feedwater line break accident. The loss of load event with delayed reactor trip establishes the minimum pressurizer POSRV capacity.

BASES

APPLICABLE SAFETY ANALYSES (continued)

The pressurizer POSRVs are components that are parts of the primary success paths and which function or actuate to mitigate a design basis event or transient that either assumes the failure of, or presents a challenge to, the integrity of a fission product barrier. As such, the pressurizer POSRVs satisfy the requirements of LCO SELECTION CRITERION 3.

LCO

The four pressurizer POSRVs are set to open at 173.7 kg/cm^{2}A (2,470 psia). The lift pressure of four POSRVs is established to prevent RCS pressure from exceeding SL and the assumed conditions of analyses. For testing the lift pressure setpoint, the upper and lower lift pressure limits for verified allowable range (As-Found Setpoint) of ±1.5 % are established based on 0.5 % of the measurement uncertainty of examination equipment plus some operating margin. After testing, however, the allowable range of setpoint (As-Left Setpoint) is adjusted within the ±0.75 % considering the change of lift setting and operating margin according to operating environmental factors.

The fully opening time is assumed the delay time of total 0.55 seconds, including the measurement uncertainty of 0.05 seconds, in the safety analyses. Therefore, the delayed opening time of the valve shall be maintained within 0.5 seconds and checked the time for refueling cycle.

If the two spring-loaded pilot valves per valve satisfy the requirements of lift setting and opening time, then it is OPERABLE status. Isolation of the main valve is limited to pertinent test valve if the verification of lift setting of spring-loaded pilot valves is performed.

The limit protected by this Specification is the reactor coolant pressure boundary SL of 110 % of design pressure and the DNBR SAFDL of 1.29.

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.

BASES

APPLICABILITY

In MODES 1, 2, and 3, and portions of MODE 4 above the LTOP temperatures, OPERABILITY of four POSRVs is required because the combined capacity is required to keep RCS 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 all pressurizer POSRVs for protection.

The LCO is not applicable in MODE 4 when all RCS cold leg temperatures are less than or equal to less than or equal to the LTOP enable temperature specified in the PTLR because LTOP protection is provided. Overpressure protection is not required in MODE 6 with the reactor vessel closure 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 pressurizer POSRVs at high pressure and temperature near their normal operating range, but only after opening time measurement and lift setting of POSRVs have had a preliminary cold setting. The cold setting gives assurance that the valves are OPERABLE near their design condition. The 72 hour exception is derived from operating experience that hot testing can be performed within this time frame.

ACTIONS

A.1

With one pressurizer POSRV inoperable, the 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 POSRV coincident with an RCS overpressure event could challenge the integrity of the RCPB.

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

If the Required Action cannot be met within the associated Completion Time, or if two or more POSRVs are inoperable, the plant must be placed in 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 all RCS cold leg temperature less than or equal to the LTOP enable temperature specified in the PTLR within 12 hours, or a condition where shutdown cooling suction line LTOP relief valves are applied within 12 hours. The 6 hours allowed is a reasonable time based on operating experience to reach MODE 3 from full power without challenging plant systems. Similarly, the 12 hours allowed is a reasonable time based on operating experience to reach MODE 4 without challenging plant systems.

ACTIONS (continued)

With 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 four POSRVs.

SURVEILLANCE REQUIREMENTS

SR 3.4.10.1

Periodic verification of the correct valve position indication in the MCR for all pressurizer POSRVs, spring-loaded pilot valves, motor operated isolation valves, manual isolation valves, and double motor operated pilot valves ensures that the valves are properly aligned and that the position indicators are functioning properly. A Frequency of 12 hours is accepted by industry practice, and has been shown to be acceptable by operating experience.

SR 3.4.10.2

Verification of correct breaker alignment and power availability to the valve position indicators ensures that valves can be operated when required, and valve positions can be monitored. Verification of removal of power to motor operated isolation valves and double motor operated pilot valves ensures that the motor operated isolation valves are not inadvertently actuated by an operator. The 7-day Frequency is accepted by industry practice and has been shown to be acceptable by operating experience.

SR 3.4.10.3

Surveillance Requirements is specified for the lift settings and opening time of pressurizer POSRVs. The allowable range of LCO to meet lift settings of POSRVs set 1.5 % of the valve setpoint and then the valve setpoint is reset within 0.75 % after refueling. ASME OM Code (Reference 2) permits the 5 years Frequency necessary to satisfy the requirements for lift settings of safety valves. However, the surveillance of the lift setting and opening time is performed every refueling cycle according to the special requirements of valves. If the two spring-loaded pilot valves per valve satisfy the requirements of lift setting and opening time, then it is OPERABLE status.

SURVEILLANCE REQUIREMENTS (continued)

SR 3.4.10.4

Verification of the OPERABILITY of alarm devices for the valve positions and electric power connections for motor operated isolation valves, manual isolation valves, and double motor operated pilot valves ensures that inadvertent actuation of each valve can be monitored. This Surveillance must be performed every 18 months.

SR 3.4.10.5

Verification of the OPERABILITY of position indicators for each valve containing main valve ensures that inadvertent actuation of each valve can be monitored. This Surveillance must be performed every 18 months.

SR 3.4.10.6

When the downstream manual isolation valves of spring-loaded pilot valves are locked in open position, overpressure protection function can be performed properly. Securing these valves in position by removing power or key locking the control in the correct position ensures that the valves cannot be inadvertently misaligned or changed position. The 18-month Frequency is based on accessibility during the refueling cycle and consideration of nuclear plant practices.

REFERENCES

1. ASME Section III.

2. ASME OM Code.

B 3.4 REACTOR COOLANT SYSTEM (RCS)

B 3.4.11 Low Temperature Overpressure Protection (LTOP) System

BASES

BACKGROUND

The purpose of the low temperature overpressure protection (LTOP) System LCO is to limit reactor coolant pressure at low temperatures to levels which will not compromise reactor coolant pressure boundary (RCPB) integrity (Reference 1). The reactor vessel is the limiting component for demonstrating that protection is provided. 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 reactor vessel neutron exposure accumulates, the vessel material toughness decreases and becomes less resistant to pressure stress at low temperatures (Reference 2). RCS pressure, therefore, is maintained low at low temperatures and is increased only as temperature is increased.

Overpressure protection given by the LCO is provided by placing the SCS suction line relief valves in service or depressurizing the reactor coolant system (RCS) through an open vent. The open RCS vent or the SCS suction line relief valves are the overpressure protection devices which provide backup to the operator in terminating increasing pressure events.

APPLICABLE SAFETY ANALYSES

Safety analyses (Reference 3) demonstrate that the reactor vessel is adequately protected against exceeding the P/T limits during shutdown. Transients that are capable of overpressurizing the RCS have been identified and evaluated. Postulated transients include inadvertent safety injection actuation; energizing the pressurizer heaters; failing the makeup control valve open; temporary loss of decay heat removal; and, reactor coolant thermal expansion caused by reactor coolant pump (RCP) start causing heat transfer from hot steam generators.

BASES

APPLICABLE SAFETY ANALYSES (continued)

The LTOP system is designed to protect the RCS from overpressurization resulting from any of the following conditions:

a. The starting of an idle RCP with the secondary water temperature of the steam generator less than or equal to 55.6 °C (100 °F) above the RCS cold leg temperature

b. The inadvertent starting of safety injection and one charging pump

LTOP System satisfies LCO SELECTION CRITERION 2.

LCO

The LCO requires that the SCS suction line relief valves be OPERABLE with a setpoint at the overpressure limit or the RCS be depressurized via an open vent.

APPLICABILITY

This LCO is applicable in MODE 4 with the temperature of any RCS cold leg less than or equal to the LTOP enable temperature specified in the PTLR during heatup, in MODE 5, and in MODE 6 with the reactor vessel head on. The LCO is not applicable for operating conditions above the specified temperatures because the POSRVs are able to provide overpressure protection. With the vessel head off, there is no need for overpressure protection

ACTIONS

A.1 and B.1

With one SCS suction line relief valve inoperable, overpressure relieving capability is reduced. The other SCS suction line relief valve remains OPERABLE or the RCS must be depressurized through an open vent. Either of these paths provides adequate overpressure protection. However, redundancy has been lost. The 7-day Completion Time in MODE 4 and 24-hour Completion Time in MODES 5 and 6 (per GL 90-06) (Reference 4) reflect the need to restore redundancy and also takes into consideration the other overpressure protection paths available in this condition.

BASES

ACTIONS (continued)

C.1

If the Required Actions cannot be met within the associated Completion Times, the plant must be placed in a condition where an overpressure event cannot occur. This is done by depressurizing the RCS through the open alternate vent. The 8-hour Completion Time is reasonable based on the amount of time required to place the plant in this condition and the probability of an accident requiring the LTOP system during this relatively short period of time.

D.1

If both SCS suction line relief valves are inoperable, an action shall be initiated to establish the alternate paths. The immediate Completion Time reflects the importance of recovering the capability of vent because the inadvertent or uncontrolled actuation of safety injection pumps or charging control valves could cause the overpressure.

SURVEILLANCE REQUIREMENTS

SR 3.4.11.1

The RCS vent must be verified open for relief protection. The required Frequency of 12 hours has been shown by operating practices to be sufficient to regularly assess degradation and verify operation within the safety analysis assumptions.

This SR is modified by a Note that states SR 3.4.11.1 is not required to be met if SR 3.4.11.2 is satisfied for LCO 3.4.11 b requirement.

SR 3.4.11.2

This SR 3.4.11.2 is the performance of a setpoint setting every 18 months. The setpoint setting for the LTOP ensures that the SCS suction line relief valves will be actuated at the appropriate RCS pressure by verifying the accuracy of the valve lift pressure. The 18-month Frequency considers operating experience with equipment reliability and matches the typical refueling cycle.

This SR is modified by a Note that states SR 3.4.11.2 is not required to be met if SR 3.4.11.1 is satisfied for LCO 3.4.11 a requirement.

REFERENCES

1. 10 CFR 50, Appendix G.
2. Generic Letter 88-11.
3. DCD Tier 2, Chapter 15.
4. Generic Letter 90-06.

B 3.4 REACTOR COOLANT SYSTEM (RCS)

B 3.4.12 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.

GDC 30 (Reference 1) requires means for detecting and, to the extent practical, identifying the source of reactor coolant LEAKAGE. NRC RG 1.45 (Reference 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 % leak tight. Leakage from these systems should be detected, located, and isolated from the containment atmosphere, if possible, to not interfere with the function of RCS leakage detection system.

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 a 1.13 L/min (0.3 gpm) primary to secondary LEAKAGE as the initial condition.

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 DCD Tier 2 (Reference 3) analysis for SGTR assumes the contaminated secondary fluid is only briefly released via safety valves and the majority is steamed to condenser. The 1.13 L/min (0.3 gpm) primary to secondary LEAKAGE is relatively inconsequential.

The SLB is more limiting for site radiation releases. The safety analysis for the SLB accident assumes the entire 1.13 L/min (0.3 gpm) primary to secondary LEAKAGE is through the affected generator as an initial condition. The dose consequences resulting from the SLB are well within the limits defined in 10 CFR 50.34.

RCS operational LEAKAGE satisfies LCO SELECTION CRITERION 2.

LCO

RCS operational LEAKAGE shall be limited to:

a. <u>Pressure boundary LEAKAGE</u>

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 gasket is not pressure boundary LEAKAGE.

LCO (continued)

b. Unidentified LEAKAGE

1.89 L/min (0.5 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 37.8 L/min (10 gpm) of identified LEAKAGE is considered allowable because LEAKAGE is from known sources which 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 sources that are specifically known and located, but does not include pressure boundary LEAKAGE or controlled RCP seal leakoff (which is a normal function and is not considered LEAKAGE). Violation of this LCO could result in continued degradation of a component or system.

LCO 3.4.13, “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 PIV line, leakage measured through one PIV may not result in any RCS LEAKAGE if the other is leak tight. If both valves leak and result in a loss of mass from the RCS, the loss must be included in allowable Identified LEAKAGE.

BASES

LCO (continued)

d. Primary-to-Secondary LEAKAGE through Any One Steam Generator

The 0.39 L/min (150 gpd) limit on primary-to-secondary LEAKAGE through any one steam generator is based on allocating the total 0.79 L/min (0.2 gpm) allowed primary-to-secondary LEAKAGE equally between the two steam generators and operational LEAKAGE performance criterion in NEI 97-06, Steam Generator Program Guidelines (Reference 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 0.39 L/min (150 gpd).” 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.

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 provided because the RCS pressure is far lower, resulting in lower stresses and a reduced potential for LEAKAGE.

ACTIONS

A.1

Unidentified LEAKAGE, identified LEAKAGE, or primary-to-secondary 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.

BASES

ACTIONS (continued)

B.1 and B.2

If any pressure boundary LEAKAGE exists or if unidentified, identified, or primary-to-secondary 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 which 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 3.4.12.1

Verifying that RCS LEAKAGE is within the LCO limits ensures that 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.

The RCS water inventory balance must be performed with the reactor at steady state operating conditions and near operating pressure. 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 level, makeup and letdown, and reactor coolant pump seal injection and return flows.

SURVEILLANCE REQUIREMENTS (Continued)

An early warning of pressure boundary LEAKAGE or unidentified LEAKAGE is provided by the automatic systems that monitor the containment atmosphere radioactivity or containment sump level. These leakage detection systems are specified in LCO 3.4.14, “RCS Leakage Detection Instrumentation.”

Note 2 states that this SR is not applicable to primary to secondary LEAKAGE because LEAKAGE of 0.39 gpm (150 gpd) 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 leak detection in the prevention of accidents.

SR 3.4.12.2

This SR verifies that primary to secondary LEAKAGE is less or equal to 0.39 L/min (150 gpd) 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 3.4.17, “Steam Generator Tube Integrity,” should be evaluated.

The 0.39 L/min (150 gpd) limit is measured at room temperature as described in Reference 5. The operational LEAKAGE rate limit applies to LEAKAGE through any one SG.

The SR 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 72-hour Frequency 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 (Reference 5).

REFERENCES

1. 10 CFR 50, Appendix A, GDC 30.

2. NRC RG 1.45, Rev. 1, May 2008.

3. DCD Tier 2, Subsection 15.6.3.

4. NEI 97-06, “Steam Generator Program Guidelines.”

5. EPRI 1022832, “Pressurized Water Reactor Primary-to-Secondary Leak Guidelines,” November 2011.

B 3.4 REACTOR COOLANT SYSTEM (RCS)

B 3.4.13 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 (References 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 3.4.12, "RCS Operational LEAKAGE." This is true during operation only when the loss of RCS mass through two valves in series is determined by an RCS water inventory balance (SR 3.4.12.1). 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 leak tight.

Although this specification provides a limit on the 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 connecting systems are degraded or becoming degraded. 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 NRC "Reactor Safety Study," WASH-1400 (Reference 4), which identified potential intersystem LOCAs as a significant contributor to the risk of core melt. A subsequent study (Reference 5) evaluated various PIV configurations to determine the probability of intersystem LOCAs.

BASES

BACKGROUND (continued)

PIVs are provided to isolate the RCS from the following typically connected systems:

a. Shutdown cooling system

b. Safety injection system

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 shutdown cooling 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 shutdown cooling system downstream of the PIVs from the RCS. Because the low pressure portion of the shutdown cooling system is typically designed for 63.2 kg/cm^{2}G (900 psig), overpressurization failure of shutdown cooling low pressure line would results 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 LCO SELECTION CRITERION 2.

LCO

RCS PIV leakage is identified LEAKAGE into closed systems connected to the RCS. PIV 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.

BASES

LCO (continued)

The LCO PIV leakage limit is 1.89 L/min (0.5 gpm) per nominal 2.54 cm (1 in) of valve size, with a maximum limit of 5 gpm (18.9 L/min). The previous criterion of 3.78 L/min (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.

Reference 6 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 powers.

APPLICABILITY

In MODES 1, 2, 3, and 4, this LCO applies because the potential for PIV leakage is greatest when the RCS is pressurized. In MODE 4, valves in the shutdown cooling flow path are not required to meet the requirements of this LCO when in, or during the transition to or from, the shutdown cooling MODE of operation.

In MODES 5 and 6, leakage limits are not provided because the RCS pressure is far lower resulting in a reduced potential for leakage and a lower potential for 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 could affect system operability or isolation of a leaking flow path with an alternate valve could degrade the ability of the interconnected system to perform its safety function.

ACTIONS (continued)

A.1 and A.2

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.

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.

The 72-hour Completion Time after exceeding the limit allows for the restoration of the leaking PIV to OPERABLE status. This time frame considers the time required to complete this Action and the low probability of a second valve failing during this period.

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 MODE 5 within 36 hours. This Action could reduce 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 SC system open permissive interlock renders the SC suction isolation valves incapable of isolating in response to a high pressure condition and preventing inadvertent opening of the valves at RCS pressure in excess of SC system design pressure. If the SC system open permissive interlock is inoperable, RCS pressure shall be depressurized below open permissive setpoint within 4 hours.

SURVEILLANCE REQUIREMENTS

SR 3.4.13.1

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 1.89 L/min (0.5 gpm) per 2.54 cm (1 in) of nominal valve diameter up to 18.9 L/min (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 could fail 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, if the plant does not go into MODE 5 for at least 72 hours. The 18-month Frequency is consistent with 10 CFR 50.55a (f) (Reference 7), as contained in the in-service testing program, is within Frequency allowed by the ASME OM Code (Reference 6), 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. Prior to returning the valve to service following maintenance, repair, or replacement work on the valve, the leak testing should be performed and the valve integrity should be verified.

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.

SURVEILLANCE REQUIREMENTS (continued)

Entry into MODES 3 and 4 is allowed to establish the necessary differential pressures and stable conditions to allow for performance of this Surveillance. Note 1 that allows this provision is complementary to the Frequency of prior to entry into MODE 2 whenever the unit has been in MODE 5 for 72 hours or more, if leakage testing has not been performed in the previous 9 months. In addition, this Surveillance is not required to be performed on the shutdown cooling system by Note 2 when the shutdown cooling system is aligned to the RCS in the shutdown cooling MODE of operation. PIVs contained in the shutdown cooling flow path must be leakage rate tested after shutdown cooling system is secured and stable unit conditions and the necessary differential pressures are established.

Note 3 that allows RCS PIVs actuated during the performance of this Surveillance are not required to be tested more than once if a repetitive testing loop cannot be avoided.

SR 3.4.13.2

The interlock setpoint that prevents the valves from being opened is set so the actual RCS pressure must be less than 31.6 kg/cm^2A (450 psia) to open the valves. This setpoint ensures that the shutdown cooling system design pressure will not be exceeded and the shutdown cooling system 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 operation experience of the equipment.

The SR is modified by a Note allowing this SR to not be met when the SCS suction isolation valves all opened for LTOP in accordance with LCO 3.4.11.a.

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. ASME OM Code.
7. 10 CFR 50.55a(f).

B 3.4 REACTOR COOLANT SYSTEM (RCS)

B 3.4.14 RCS Leakage Detection Instrumentation

BASES

BACKGROUND

GDC 30 of Appendix A to 10 CFR 50 (Reference 1) requires means for detecting and, to the extent practical, identifying the location of the source of RCS leakage. NRC RG 1.45 (Reference 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. In addition, to meet the OPERABLE requirements, the monitors are typically set to provide the most sensitive response without causing an excessive number of spurious alarms.

The containment sump used to collect unidentified leakage and the containment atmosphere humidity monitor is instrumented to alarm for increases of above in the normal rates.

The reactor coolant contains radioactivity that, when released to the containment, can be detected by radiation monitoring instrumentation. Radioactivity detection systems are included for monitoring the particulate activity, because of its sensitivities and rapid responses to RCS leakage.

Other indications may be used to detect an increase in unidentified leakage. However, they are not required to be OPERABLE by this LCO. 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.

Since the humidity level is influenced by several factors, a quantitative evaluation of an indicated leakage rate by this means could be questionable and should be compared to observed increases in liquid flow into or from the containment sump and atmosphere humidity monitor.

BASES

BACKGROUND (continued)

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 could indicate RCS leakage into the containment. The relevance of temperature and pressure measurements is 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.

The above mentioned leakage detection methods or systems differ in sensitivity and response time. Some of these systems could serve as early alarm systems signaling the operators that closer examination of other detection systems is necessary to determine the extent of any corrective action that could be required.

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 the indications from other systems is necessary.

The safety significance of RCS leakage varies widely depending on its source, rate, and duration. Therefore, detecting and monitoring of RCS leakage into the containment area is 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).

LCO

This LCO requires instruments of diverse monitoring principles to be OPERABLE to provide confidence that small amounts of unidentified leakage are detected in time to allow actions to place the plant in a safe condition when RCS leakage indicates possible RCPB degradation.

The LCO requires three instruments to be OPERABLE.

The containment sump is used to collect unidentified leakage. The containment sump consists of the normal sump and ICI cavity sump. The LCO requirements apply to the total amount of unidentified leakage collected in the both sumps. The monitor on the measuring tube inside the containment sump detects the leakage level or the operating frequency of discharge in the measuring tube inside containment sump. The measuring tube is instrumented to detect when there is leakage of an increase above the normal value by 0.5 gpm. The identification of an increase in unidentified leakage will be delayed by the time required for the unidentified leakage to travel to the containment sump and it could take longer than 1 hour to detect a 0.5 gpm increase in unidentified leakage, depending on the origin and magnitude of the leakage. This sensitivity is acceptable for containment sump monitor OPERABILITY.

The reactor coolant contains radioactivity that, when released to the containment, can be detected by the particulate containment atmosphere radioactivity monitor. Radioactivity detection systems are included for monitoring particulate activities because of its sensitivities and rapid responses to RCS leakage, but have recognized limitations. The reactor coolant radioactivity level 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.

If there are few fuel element cladding defects and low levels of activation products, it may not be possible for the particulate containment atmosphere radioactivity monitor to detect a 0.5 gpm increase within 1 hour during normal operation. However, the particulate containment atmosphere radioactivity monitor is OPERABLE when it is capable of detecting a 0.5 gpm increase in unidentified leakage within 1 hour given an RCS activity equivalent to that assumed in the design calculations for the monitors (Reference 3).

BASES

LCO (continued)

An increase in humidity of the containment atmosphere could indicate the release of water vapor to the containment. Containment humidity is instrumented to detect when there is an increase above the normal value by 1 gpm. The time required to detect a 1 gpm increase above the normal value various based on environmental and system conditions and could take longer than 1 hour. This sensitivity is acceptable for containment atmosphere humidity monitor OPERABILITY.

The LCO is satisfied when monitors of diverse measurement means are available. Thus, the combination of containment sump monitors, in combination with a particulate radioactivity monitor and humidity monitors 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 MODES 5 or 6, the temperature is less than or equal to 98.9 °C (210 °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

With the required 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 containment atmosphere radioactivity monitor, the periodic surveillance for the RCS water inventory balance, SR 3.4.12.1, 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 3.4.12.1 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 stable plant conditions are established.

ACTIONS (continued)

Restoration of the required sump monitor to OPERABLE status within a Completion Time 31 days is required to regain the function 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.

B.1.1, B.1.2, B.2.1, and B.2.2

With the particulate containment atmosphere radioactivity monitoring instrumentation channel 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 3.4.12.1, must be performed to provide alternate periodic information.

With a sample obtained and analyzed or water inventory balance performed every 24 hours, the reactor may be operated for up to 31 days to allow restoration of the required containment atmosphere radioactivity monitors. Alternatively, continued operation is allowed if the containment atmosphere humidity monitor is OPERABLE, provided grab samples are taken or water inventory balances performed every 24 hours.

The 24-hour interval provides periodic information that is adequate to detect leakage. A Note is added allowing that SR 3.4.12.1 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 31-day Completion Time recognizes at least one other form of leakage detection is available.

C.1 and C.2

With the containment atmosphere humidity monitor inoperable, alternative action is again required. Either SR 3.4.14.1 must be performed or water inventory balance, in accordance with SR 3.4.12.1, must be performed to provide alternate periodic information. Provided a CHANNEL CHECK is performed every 8 hours, or a water inventory balances is performed every 24 hours, reactor operation may continue while awaiting restoration of the containment atmosphere humidity monitor to OPERABLE status. The 24-hour interval provides periodic information that is adequate to detect RCS leakage.

ACTIONS (continued)

A Note is added allowing that SR 3.4.12.1 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.

D.1, D.2.1 and D.2.2

With the required containment sump monitor and the containment atmosphere humidity monitor inoperable, the only means of detecting LEAKAGE is the required containment atmosphere radiation monitor. A Note clarifies that this condition is applicable when the only OPERABLE monitor is the containment atmosphere radioactivity monitor. The containment atmosphere radioactivity monitor typically cannot detect a 0.5 gpm leak within one hour when RCS activity is low. In addition, this configuration does not provide the required diverse means of leakage detection. Indirect methods of monitoring RCS leakage must be implemented. Grab samples of the containment atmosphere must be taken to provide alternate periodic information. The 12-hour interval is sufficient to detect increasing RCS leakage. The Required Action provides 7 days to restore another RCS leakage monitor to OPERABLE status to regain the intended leakage detection diversity. The 7-day Completion Time ensures that the plant will not be operated in a degraded configuration for a lengthy time period.

E.1 and E.2

With the required containment atmosphere radioactivity monitor and the containment atmosphere humidity monitor 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 required monitors to OPERABLE status within 31 days to regain the intended leakage detection diversity. The 31-day Completion Time ensures that the plant will not be operated in a reduced configuration for a lengthy time period.

BASES

ACTIONS (continued)

F.1 and F.2

If a Required Action of Condition A, B, C, D or E cannot be met, 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 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

If all required monitors 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 3.4.14.1

SR 3.4.14.1 requires the performance of a CHANNEL CHECK of the required containment atmosphere radioactivity monitors. The check gives reasonable confidence that the channel is operating properly. The Frequency of 12 hours is based on instrument reliability and is reasonable for detecting off normal conditions.

SR 3.4.14.2

SR 3.4.14.2 requires the performance of a CHANNEL FUNCTIONAL TEST on the required containment atmosphere radioactivity monitor. The test ensures that the monitor can perform its function in the desired manner. 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 (TS) and non-TS tests at least once per refueling interval with applicable extensions. The test verifies the alarm setpoint and relative accuracy of the instrument string. The Frequency of 31 days considers instrument reliability, and operating experience has shown that it is proper for detecting degradation.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.4.14.3, SR 3.4.14.4, and SR 3.4.14.5

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 18-month frequency is a typical refueling cycle and considers channel reliability. Again, operating experience has proven that this Frequency is acceptable.

REFERENCES

1. 10 CFR 50, Appendix A, Section IV, GDC 30.
2. NRC RG 1.45, Rev. 1, May 2008
3. DCD Tier 2, Chapter 5.

B 3.4 REACTOR COOLANT SYSTEM (RCS)

B 3.4.15 RCS Specific Activity

BASES

BACKGROUND

The maximum dose that an individual at the exclusion area boundary can receive for 2 hours following an accident, or at low population zone outer boundary for the radiological release duration, is specified in 10 CFR 50.34 (Reference 1). Doses to main control room (MCR) operators must be limited per GDC 19. The limits on specific activity ensure that the offsite and MCR doses are appropriately limited 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 dose consequences in the event of a steam line break (SLB) or a steam generator tube rupture (SGTR) accident.

The LCO contains specific activity limits for both DOSE EQUIVALENT I-131 and DOSE EQUIVALENT XE-133. The allowable levels are intended to ensure that offsite and MCR doses meet the appropriate acceptance criteria in the Standard Review Plan (Reference 2).

APPLICABLE SAFETY ANALYSES

The LCO limits on the specific activity of the reactor coolant ensures that the resulting offsite and MCR doses meet the appropriate SRP acceptance criteria following a SLB or a SGTR accident. The safety analyses (Reference 3 and 4) assume the specific activity of the reactor coolant is at the LCO limits, and an existing reactor coolant steam generator (SG) tube leakage rate of 2.27 L/min (0.6 gpm) exists. The safety analyses assume the specific activity of the secondary coolant is at its limit of 3.70×10^3 Bq/g DOSE EQUIVALENT I-131 from LCO 3.7.17, “Secondary Specific Activity”.

The analyses for the SLB and SGTR accidents establish the acceptance limits for RCS specific activity. Reference to these analyses is used to assess changes to the unit that could affect RCS specific activity, as they relate to the acceptance limits.

APPLICABLE SAFETY ANALYSES (continued)

The safety analyses consider two cases of reactor coolant iodine specific activity. One case assumes specific activity at 3.70 x 10^4 Bq/g DOSE EQUIVALENT I-131 with a concurrent large iodine spike that increases the rate of release of iodine from the fuel rods containing cladding defects to the primary coolant immediately after a SLB (by a factor of 500), or SGTR (by a factor of 335), respectively. The second case assumes the initial reactor coolant iodine activity at 2.22 x 10^6 Bq/g DOSE EQUIVALENT I-131 because of an iodine spike caused by a reactor or an RCS transient prior to the accident. In both cases, the noble gas specific activity is assumed to be 1.11 x 10^7 Bq/g DOSE EQUIVALENT XE-133.

The SGTR analysis assumes a 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 and the Shutdown Cooling (SC) system is placed in service.

The SLB radiological analysis assumes that offsite power is lost at the same time as the pipe break occurs outside containment. The affected SG blows down completely and steam is vented directly to the atmosphere. The unaffected SG removes core decay heat by venting steam to the atmosphere until the cooldown ends and the SC system is placed in service.

Operation with iodine specific activity levels greater than the LCO limit is permissible, if the activity levels do not exceed 2.22 x 10^6 Bq/g for more than 48 hours.

The limits on RCS specific activity are also used for establishing standardization in radiation shielding and plant personnel radiation protection practices.

RCS specific activity satisfies LCO SELECTION CRITERION 2.

BASES

LCO

The iodine specific activity in the reactor coolant is limited to 3.70 x 10^4 Bq/g DOSE EQUIVALENT I-131, and the noble gas specific activity in the reactor coolant is limited to 1.11 x 10^7 Bq/g DOSE EQUIVALENT XE-133. The limits on specific activity ensure that offsite and MCR doses will meet the appropriate SRP acceptance criteria (Reference 2).

The SLB and SGTR accident analyses (References 3 and 4) show that the calculated doses are within acceptable limits. Violation of the LCO could result in reactor coolant radioactivity levels that could, in the event of a SLB or SGTR, lead to doses that exceed the SRP acceptance criteria (Reference 2).

APPLICABILITY

In MODES 1, 2, 3 and 4, operation within the LCO limits for DOSE EQUIVALENT I-131 and DOSE EQUIVALENT XE-133 is necessary to limit the potential consequences of a SLB or SGTR to within the SRP acceptance criteria (Reference 2).

In MODES 5 and 6, the steam generators are not being used for decay heat removal, the RCS and steam generators are depressurized, and primary to secondary leakage is minimal. Therefore, the monitoring of RCS specific activity is not required.

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 that the specific activity is less than or equal to 2.22 x 10^6 Bq/g. The Completion Time of 4 hours is required to obtain and analyze a sample. Sampling is continued every 4 hours to provide a trend.

The DOSE EQUIVALENT I-131 must be restored to within limit within 48 hours.

The Completion Time of 48 hours is acceptable since it is expected that, if there were an iodine spike, the normal coolant iodine concentration would be restored within this time period. Also, there is a low probability of a SLB or SGTR occurring during this time period.

ACTIONS (continued)

A Note excludes the MODE change restriction of LCO 3.0.4. This exception allows entry into the applicable MODE(s), relying on Required Actions A.1 and A.2 while the DOSE EQUIVALENT I-131 LCO limit is not met. This exception 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

With the DOSE EQUIVALENT XE-133 greater than the LCO limit, DOSE EQUIVALENT XE-133 must be restored to within limit within 48 hours. The allowed Completion Time of 48 hours is acceptable since it is expected that, if there were a noble gas spike, the normal coolant noble gas concentration would be restored within this time period. Also, there is a low probability of a SLB or SGTR occurring during this time period.

A Note excludes the MODE change restriction of LCO 3.0.4. This exception allows entry into the applicable MODE(s), relying on Required Actions B.1 while the DOSE EQUIVALENT XE-133 LCO limit is not met. This exception 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.

C.1 and C.2

If the Required Action and the associated Completion Time of Condition A or B is not met, or if the DOSE EQUIVALENT I-131 is greater than 2.22×10^6 Bq/g, the reactor must be brought to MODE 3 within 6 hours and MODE 5 within 36 hours. The allowed Completion Time is 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 3.4.15.1

SR 3.4.15.1 requires performing a gamma isotopic analysis as a measure of the noble gas specific activity of the reactor coolant at least once every 7 days. 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 the noble gas 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 7-day Frequency considers the low probability of a gross fuel failure during the time.

Due to the inherent difficulty in detecting Kr-85 in a reactor coolant sample due to masking from radioisotopes with similar decay energies, such as F-18 and I-134, it is acceptable to include the minimum detectable activity for Kr-85 in the SR 3.4.15.1 calculation. If a specific noble gas nuclide listed in the definition of DOSE EQUIVALENT XE-133 is not detected, it should be assumed to be present at the minimum detectable activity.

A Note modifies the SR to allow entry into and operation in MODE 4, MODE 3, and MODE 2 prior to performing the SR. This allows the Surveillance to be performed in those MODES, prior to entering MODE 1.

SR 3.4.15.2

This Surveillance is performed to ensure iodine specific activity remains within the LCO limit during normal operation and following fast power changes when iodine spiking is more apt to occur. The 14-day Frequency is adequate to trend changes in the iodine activity level, considering noble gas activity is monitored every 7 days. The Frequency, between 2 and 6 hours after a power change greater than or equal to 15 % RTP within a 1-hour period, is established because the iodine levels peak during this time following iodine spike initiation; samples at other times would provide inaccurate results.

The Notes modifies this SR to allow entry into and operation in MODE 4, MODE 3, and MODE 2 prior to performing the SR. This allows the Surveillance to be performed in those MODES, prior to entering MODE 1.

REFERENCES

1. 10 CFR 50.34.
2. NUREG-0800, Section 15.0.3, March 2007.
3. DCD Tier 2, Subsection 15.1.5.
4. DCD Tier 2, Subsection 15.6.3.

B 3.4 REACTOR COOLANT SYSTEM (RCS)

B 3.4.16 Reactor Coolant Gas Vent (RCGV) function

BASES

BACKGROUND

The reactor coolant gas vent (RCGV) function is to provide a safety grade means of venting non-condensible gases and steam from the pressurizer and the reactor vessel closure head. The RCGV function is designed to be used during all design bases events for RCS pressure control purposes when main spray and auxiliary spray systems are unavailable. The OPERABILITY of at least one RCGV path from the pressurizer and at least one RCGV path from the reactor vessel closure head to the RDT or the IRWST ensures that this function can be performed.

The RCGV function is a manually operated safety grade system. It removes non-condensible gases or steam from the pressurizer and the reactor vessel closure head through vent lines to the RDT or IRWST. Each vent line has two pairs of parallel isolation valves which are closed during normal operation. During shutdown or transient conditions, if the operator judges that non-condensible gases are collected in the pressurizer or in the reactor vessel closure head, the operator vents the gases by manually opening the RCGV valves from the MCR according to operating procedures. The RCGV function will have the capability to be manually actuated, monitored, and controlled from the MCR as required by GDC 19.

The two isolation valves in each parallel path are normally powered from the 125Vdc buses and emergency power is provided to the valves by batteries. A failure modes and effect analysis (FMEA) (Reference 1) demonstrates that the RCGV function will maintain a vent path after a single failure of any single valve or its power source. This demonstration satisfies the requirements of GDC 17 and GDC 34.

APPLICABLE SAFETY ANALYSES

The RCGV function provides a safety grade method of RCS depressurization that is credited during natural circulation and during steam generator tube rupture events. The operator uses the SI System, the pressurizer backup heaters, and the RCGV function to control RCS inventory and subcooling. The pressurizer vent line is 5.0 cm (2.0 in) nominal diameter to meet the requirement to vent one-half the RCS volume in one hour.

BASES

APPLICABLE SAFETY ANALYSES (continued)

The reactor vessel vent line is a 1.9 cm (3/4 in) line which expands to 2.54 cm (1 in) through the valving. This provides adequate venting to remove steam and non-condensible gases from the reactor vessel closure head.

The RCGV function satisfies LCO SELECTION CRITERION 3.

LCO

The purpose of the LCO is to ensure the core cooldown and RCS depressurization can be established using natural circulation venting non-condensible gases from the reactor vessel upper closure head and the pressurizer steam space at post-accident conditions. The RCGV function is OPERABLE when a vent path can be established from the pressurizer steam space and from the reactor vessel closure head to the RDT or IRWST. The valves are designed to be closed when the solenoid valves are de-energized to minimize the possibility of the common failure, and powered from the division A and B with different power sources, respectively.

This LCO is to ensure the capability of core cooldown and RCS depressurization, therefore, establishes the OPERABLE vent paths from the reactor vessel closure head and the pressurizer steam space to the RDT or IRWST, and ensure the independent power for valves in vent paths.

APPLICABILITY

In MODES 1, 2, 3, and in MODE 4 with RCS pressure greater than or equal to 31.6 kg/cm^{2}A (450 psia), the two vent paths of the reactor vessel closure head and the pressurizer are required to be OPERABLE. The RCGV function is primarily used for natural circulation and for steam generator tube rupture events considering loss of offsite power and single failure events. It assumes the pressurizer auxiliary spray system is inoperable when these events occur. Vent paths of the reactor vessel closure head and the pressurizer steam space are used as the means of RCS depressurization. In MODES 1, 2, 3, and in MODE 4 with RCS pressure greater than or equal to 31.6 kg/cm^{2}A (450 psia), the steam generators are primarily used for RCS heat removal up to a point of the time before starting shutdown cooling system.

In MODES 1, 2, 3, and in MODE 4 with RCS pressure greater than or equal to 31.6 kg/cm^{2}A (450 psia), vent valves of the reactor vessel closure head and the pressurizer are used for RCS depressurization up to a point of the time before entering shutdown cooling when the pressurizer auxiliary spray system is inoperable.

APPLICABILITY (continued)

The OPERABLE RCS vent paths are not required for operating shutdown cooling system because the overpressure protection of the RCS is performed by the LTOP system.

In MODES 5 and 6, there is no need for OPERABLE RCS vent paths since the RCS temperature is low and depressurized enough.

ACTIONS

The ACTIONS are modified by a Note which is added to provide clarification that each RCS gas vent path of the reactor vessel closure head and the pressurizer steam space allows a separate entry into a Condition.

A.1

With inoperable components, such that one required vent path is inoperable, the required vent path must be returned to OPERABLE status within 72 hours. The Completion Time of 72 hours is a reasonable considering OPERABLE status of the other vent path.

B.1

With components inoperable, such that two required vent paths from either location are inoperable, at least one of the vent paths must be returned to OPERABLE status within 6 hours.

The Completion Time of 6 hours is reasonable to allow time to correct the situation, considering the importance of restoring at least one vent path. If at least one vent path is not restored to OPERABLE within 6 hours, then Required Action C is entered.

C.1 and C.2

If the Required Action and associated Completion Time of Condition A or B 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 in MODE 3 within 6 hours, and then in MODE 4 with RCS pressure less than 31.6 kg/cm^{2}A (450 psia) within 12 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.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.4.16.1

At least one complete cycling for all remote control valves in each vent path from the MCR verifies the RCGV function valves will function when necessary. The Surveillance test must be performed in MODE 5 or 6. The 18-month Frequency is based on a typical refueling cycle and industry accepted practice.

SR 3.4.16.2

This SR requires verification of flow through each vent path and the Surveillance test must be performed in MODE 5 or 6. The Surveillance is performed during venting. The 18-month Frequency is based on a typical refueling cycle and is an industry accepted practice.

SR 3.4.16.3

There is one locally operated manual valve for the RCGV function in the vent path from the reactor vessel closure head. It is necessary to verify that this valve is locked open to ensure that a vent path can be established from the reactor vessel closure head to the RDT or IRWST. The Surveillance test must be performed in MODE 5 or 6. The 18-month Frequency is based on accessibility during the refueling cycle and industry accepted practice.

SR 3.4.16.4

Verification of the correct breaker alignment and valve position indication ensures that the valves are able to actuate and the valve positions are able to be monitored when necessary. The 7-day Frequency has been shown to be acceptable by operating experience.

REFERENCES

1. DCD Tier 2, Subsection 5.4.12.

B 3.4 REACTOR COOLANT SYSTEM (RCS)

B 3.4.17 Steam Generator 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 can 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.

BASES

BACKGROUND (continued)

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 (Reference 1).

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 3.4.12, “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 relief valves.

The analysis for design basis accidents and transients other than a SGTR assume the SG tubes retain their structural integrity (i.e., do not rupture.) In these analyses, the steam discharge to the atmosphere is based on the total primary to secondary leakage from all SGs of 1.13 L/min (0.3 gpm). 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 3.4.15, “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 (Reference 2), 10 CFR 100 (Reference 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 in accordance with the Steam Generator Program.

During an SG inspection, any inspected tube that satisfies the Steam Generator Program repair criteria is removed from service by plugging. If a tube was determined to satisfy the repair criteria but was not plugged, the tube may still have tube integrity.

LCO (Continued)

In the context of this Specification, a SG tube is defined as the entire length of the tube, including the tube wall, 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.

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.

LCO (Continued)

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 (Reference 4) and NRC RG 1.121 (Reference 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 0.39 L/min (150 gpd) 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.

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 3.4.12, “RCS Operational Leakage,” and limits primary to secondary leakage through any one SG to 0.39 L/min (150 gpd). 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.

A.1 and A.2

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 in accordance with the Steam Generator Program as required by SR 3.4.17.2. 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 Tube Surveillance 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 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 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 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.

BASES

ACTIONS (continued)

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 3.4.17.1

During shutdown periods the SGs are inspected as required by this SR and the Steam Generator Program. NEI 97-06, Steam Generator Program Guidelines (Reference 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.

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, nondestructive examination (NDE) technique capabilities, and inspection locations.

The Steam Generator Program defines the Frequency of SR 3.4.17.1. 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.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.4.17.2

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.

REFERENCES

1. NEI 97-06, “Steam Generator Program Guidelines.”
2. 10 CFR 50, Appendix A, GDC 19.
3. 10 CFR 100.
4. ASME Section III, Subsection NB.
5. NRC RG 1.121, August 1976.
6. EPRI 1022832, “Pressurized Water Reactor Steam Generator Examination Guidelines,” November 2011.

B 3.5 EMERGENCY CORE COOLING SYSTEM (ECCS)

B 3.5.1 Safety Injection Tanks (SITs)

BASES

BACKGROUND

The functions of the four safety injection tanks (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 and gravity are sufficient to discharge the contents to the RCS, if RCS pressure decreases below the SIT pressure.

Each SIT discharges its water volume directly to the reactor vessel downcomer via a direct vessel injection (DVI) nozzle, also used by the safety injection system (SIS). 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.

BACKGROUND (continued)

Additionally, the isolation valves are interlocked with the pressurizer pressure instrumentation channels to ensure the valves will automatically open as RCS pressure is increased above SIT pressure and to prevent inadvertent closure prior to an accident. The valves also receive a safety injection actuation signal (SIAS) from the plant protection system (PPS) or diverse protection system (DPS) to open. These features ensure the valves meet the requirements of IEEE Std. 603-1991 (Reference 1) for "operating bypasses" and that the SITs will be available for injection without reliance on operator action.

The SIT gas and water volumes, gas pressure, and outlet pipe size are selected to allow 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 DVI line break assumption and that four SITs is consistent with cold leg break assumption in the LOCA analysis.

APPLICABLE SAFETY ANALYSES

The SITs are taken credit for in both the large and small break LOCA analysis at full power (Reference 2). 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 safety injection 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 safety injection pumps cannot deliver flow until the emergency diesel generators (EDGs) start, come to rated speed, and go through their timed loading sequence. In LOCA, the entire contents of four SITs are assumed to be injected directly to vessel downcomer via the direct vessel injection nozzle during blowdown.

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 below SIT pressure.

APPLICABLE SAFETY ANALYSES (continued)

As a conservative estimate in the calculation of the reflood portion of the accident, no credit is taken for safety injection pump flow until the SITs 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 40 seconds. No operator action is assumed during blowdown stage of a large break LOCA.

The worst case small break LOCA assumes also some 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 mainly by the SITs, with pumped flow then providing continued cooling. As break size continues to decrease, the SITs and an SI pump both play a part in terminating the rise in clad temperature. As break size decreases the role of the SITs decreases until they are not required and the SI 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 (Reference 3) for emergency core cooling systems (ECCS), will be met following a LOCA:

a. Maximum fuel element cladding temperature of less than or equal to 1,204.4 °C (2,200°F)

b. Maximum cladding oxidation of less than or equal to 0.17 times the total cladding thickness before oxidation

c. Maximum hydrogen generation from a zirconium-water reaction of less than or equal to 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

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 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.

APPLICABLE SAFETY ANALYSES (continued)

These precautions ensure that the SITs are available during an accident (Reference 4). 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 a DVI break only two SITs would reach the core. Since the only active failure which 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 four SITs can provide adequate inventory to reflood the core and downcomer following a LBLOCA. The downcomer then remains flooded until the Safety Injection Pumps start to deliver flow.

The maximum volume limit is based upon 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.

A minimum of 25 % narrow range level corresponding to 50.7 m^3 (1,790 ft^3) of borated water, and a maximum of 75 % narrow range level corresponding to 54.6 m^3 (1,927 ft^3) of borated water, are used in the safety analyses as the volume in the SITs. To allow for instrument accuracy, 29 % narrow range (corresponding to 51.1 m^3 (1,805 ft^3)) and 69 % narrow range (corresponding to 54.0 m^3 (1,906 ft^3)), are specified. The analyses are based upon the cubic feet requirements; the percentage figures are provided for operator use because the level indication provided in the MCR is in percentages, not in cubic feet.

The minimum nitrogen gas pressure requirement ensures that the contained gas volume will generate discharge flow rates during injection which are consistent with those assumed in the safety analyses.

The maximum nitrogen cover gas pressure limit ensures that excessive amounts of gas will not be injected into the RCS after the SITs have emptied.

A minimum pressure of 40.1 kg/cm^2G (570 psig) and a maximum pressure of 44.4 kg/cm^2G (632 psig) are used in the analyses. To allow for instrument accuracy, a 40.6 kg/cm^2G (578 psig) minimum and 43.9 kg/cm^2G (624 psig) maximum are specified.

APPLICABLE SAFETY ANALYSES (continued)

The maximum allowable boron concentration of 4,400 ppm in the SITs 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 leg and DVI nozzle injection are based upon the worst case minimum boron precipitation time. Maintaining the maximum SIT boron concentration within the upper limit ensures 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 2,300 ppm are based on beginning of life reactivity values and are selected to ensure 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 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 in-containment refueling water storage tank (IRWST) the minimum SIT concentration is lower than the IRWST. Dilution by the RCS was already taken into account for in the calculation of the minimum boron requirements for the SITs. Operators need not account for dilution by the RCS.

The SITs satisfy LCO Selection Criterion 3.

LCO

The LCO establishes the minimum conditions required to ensure the SITs are available to accomplish their core cooling safety function following a LOCA. Four SITs are required OPERABLE to ensure 100 % of the contents of four of the SITs will reach the core during a LBLOCA.

If the contents of fewer than four tanks are injected during the blowdown phase of a LOCA, the ECCS acceptance criteria of 10 CFR 50.46 (Reference 3) could be violated.

BASES

LCO (continued)

For a SIT to be considered OPERABLE, the motor operated isolation valve must be fully open with power removed and the limits established in the SR for contained volume, boron concentration and nitrogen cover gas pressure must be met.

APPLICABILITY

In MODES 1 and 2, and MODES 3 and 4 with RCS pressure greater than or equal to 50.3 kg/cm^{2}A (715 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 greater than or equal to 50.3 kg/cm^{2}A (715 psia). Below 50.3 kg/cm^{2}A (715 psia), the rate of RCS blowdown is such that the SI pumps can provide adequate injection to ensure that peak clad temperature remains below the 10 CFR 50.46 (Reference 3) limit of 1,204.4 °C (2,200°F).

In MODES 3 and 4 with pressure less than 50.3 kg/cm^{2}A (715 psia) and in MODES 5 and 6, the SIT motor-operated isolation valves are closed to isolate the SITs from RCS. This allows RCS cooldown and depressurization without discharging the SITs into the RCS or requiring depressurization of the SITs.

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 could 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 four 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.

ACTIONS (continued)

B.1

If the level and pressure cannot be verified, pressure and level indication for the affected SIT would not be available to the Operators. However, in this condition the SIT would still be available to fulfill its function because it is unlikely that the level or pressure would deteriorate to outside specified limits within 72 hours. Therefore, based on this, and that the level and pressure instrumentation associated with the SITs do not initiate a safety action, it is reasonable to allow 72 hours to restore the SIT to OPERABLE status. This is consistent with the recommendations of NUREG-1366 (Reference 5).

If there is a known condition where pressure or level could not be maintained within limits for at least 72 hours, then the affected SIT would be considered inoperable for reasons other than the inability to verify level or pressure.

C.1

If one SIT is inoperable, for a reason other than boron concentration or the inability to verify level or pressure, the SIT must be returned to OPERABLE status within 1 hour. In this Condition, the required contents of four SITs cannot be assumed to reach the core during a LBLOCA. Due to the severity of the consequences should a LOCA occur in these conditions, the 1-hour Completion Time to open the valve, remove power to the valve, or restore the proper water volume or nitrogen cover gas pressure ensures that prompt action will be taken to return the inoperable SIT to OPERABLE status. The Completion Time minimizes the exposure of the plant to a LOCA in these conditions.

D.1 and D.2

If the SIT cannot be returned to OPERABLE status within the associated Completion Time, the plant must be placed in 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 less than 50.3 kg/cm^{2}A (715 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.

ACTIONS (continued)

E.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 MCR, ensures the 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 position should not change 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 gas pressure should be verified to 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 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.

SR 3.5.1.4

A period of 31 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 which could occur from mechanisms such as stratification or in-leakage. Sampling the affected SIT will identify whether inleakage from the RCS 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 IRWST, because the water contained in the IRWST is within the SIT boron concentration requirements. This is consistent with the recommendations of NUREG-1366 (Reference 5).

SURVEILLANCE REQUIREMENTS (continued)

SR 3.5.1.5

Verification every 31 days that power is removed from each SIT isolation valve operator when the pressurizer pressure is greater than or equal to 50.3 kg/cm^{2}A (715 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 three SITs would be available for injection during 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 pressurizer pressure is less than 50.3 kg/cm^{2}A (715 psia), thus allowing operational flexibility by avoiding unnecessary delays to manipulate the breakers during unit startups or shutdowns. Even with power supplied to the valves, inadvertent closure is prevented by the RCS pressure interlock associated with the valves. Should closure of a valve occur in spite of the interlock, the SI signal provided to the valves would open a closed valve in the event of a LOCA.

REFERENCES

1. IEEE Standard 603-1991.
2. DCD Tier 2, Chapter 6.
3. 10 CFR 50.46.
4. DCD Tier 2, Chapter 15.
5. NUREG-1366, February 1990.

B 3.5 EMERGENCY CORE COOLING SYSTEM (ECCS)

B 3.5.2 Safety Injection System (SIS) – Operating

BASES

BACKGROUND

The function of the SIS 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

d. Steam generator tube rupture (SGTR)

The addition of negative reactivity is designed primarily for the steam line break accident where primary cooldown could add enough positive reactivity to achieve criticality and return to significant power.

There is only one phase of SIS operation. In the injection phase, all injection is added to the reactor coolant system (RCS) via the direct vessel injection (DVI) nozzles. After the blowdown stage of the LOCA stabilizes, injection flow is split equally between the hot legs and DVI nozzles.

Four mechanically redundant safety injection (SI) trains are provided. Each train consists of an SI pump and the associated piping and valves. SI flow credited in LOCA analyses is dependent on the pipe break location. Full flow from two[(1)] pumps and four SITs is credited for a break in an RCP discharge leg. Full flow from one SI pump and three SITs is credited for a break in a DVI line; the flow from the one pump and from one SIT is assumed to spill out the break. In MODES 1, 2, and 3, all SI trains are required to be OPERABLE. This ensures that 100 % of the core cooling requirements can be provided even in the event of a RCP discharge leg break or a DVI line break with a failure of emergency diesel generator (EDG) to start.

(1) The two injection lines corresponding to the two inoperable trains are diagonal in reactor vessel (i.e., SI train# 1/3 or 2/4).

BACKGROUND (continued)

An independent suction header supplies water from the in-containment refueling water storage tank (IRWST) to each of the safety injection pumps. Each SI pump discharges directly to the reactor vessel downcomer via the direct vessel injection nozzle. The SI pump directs sufficient flow to the core to meet the analysis assumptions following a loss of coolant accident (LOCA) in one of the RCS cold legs.

During a large break LOCA RCS pressure will decrease to less than 14.1 kg/cm^{2}A (200 psia) in less than 20 seconds. The safety injection (SI) systems are actuated upon receipt of an SIAS from PPS or DPS. 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 features (ESF) buses shed normally operating loads and are connected to the emergency diesel generators (EDGs). 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 SIS components, along with the passive safety injection tanks (SITs) and the IRWST, covered in LCO 3.5.1, “Safety Injection Tanks (SITs),” and LCO 3.5.4, “In-containment Refueling Water Storage Tank (IRWST),” provide the cooling water to meet GDC 35 (Reference 1).

APPLICABLE SAFETY ANALYSES

LCO 3.5.2 helps to ensure that the following acceptance criteria established by 10 CFR 50.46 (Reference 2) for SIS will be met following a LOCA:

a. Maximum fuel element cladding temperature of less than or equal to 1,204.4 °C (2,200 °F)

b. Maximum cladding oxidation of less than or equal to 0.17 times the total cladding thickness before oxidation

c. Maximum hydrogen generation from a zirconium-water reaction of less than or equal to 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

APPLICABLE SAFETY ANALYSES (continued)

d. The core is maintained in a coolable geometry.

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) accident and a CEA ejection accident and ensure that containment temperature limits are met.

SI pump flow is set during pre-operational testing to ensure that the pump runout flow is not excessive when the RCS is at atmospheric conditions. The SI system is assumed to be OPERABLE in the large break and small break LOCA analyses at full power, DCD Tier 2, Chapter 6 (Reference 3). The delivered SI pump flow credited in safety analyses for a LOCA is dependent on the pressure conditions that exist as a result of the size of the LOCA. SI delivery curves define the SI performance credited in the large and small break LOCA analyses over the operating range of the SI pumps from pump shutoff head to pump runout flow. The main steam line break accident also establishes the flow-head requirement and in addition establishes the minimum required response time for actuation of the pumps. The steam generator tube rupture (SGTR), CEA ejection, and inadvertent opening of an atmospheric dump valve analyses also credit the SI pumps, but do not limit the design.

The large break LOCA event with a loss of offsite power and a single failure (disabling one SIS train) establishes the OPERABILITY requirements for the SIS. 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 CEA insertion during small breaks. Long-term shutdown is preserved by the borated water delivered by the SIS to the core. Following depressurization, emergency cooling water is injected through the direct vessel injection nozzles, 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 and the lower the injection flow rate. In all LOCA analyses, injection flow is not credited until RCS pressure drops below the shutoff head of the SI pumps.

BASES

APPLICABLE SAFETY ANALYSES (continued)

The LCO ensures an SIS train will deliver sufficient water to match decay heat boil-off rates soon enough to minimize core uncovery for a large LOCA.

It also ensures that the SI pump will deliver sufficient water during a small break LOCA, and provide sufficient boron, in conjunction with the CEA's (assuming that the most reactive CEA does not insert), to maintain the core subcritical following an SLB.

SIS – Operating satisfies LCO Selection Criterion 3.

LCO

In MODES 1, 2, and 3, four independent (and redundant) SIS trains are required to ensure sufficient SIS flow is available to mitigate the consequences of a LOCA assuming a single failure coincident with a LOOP. Additionally, the SIS trains may be called upon to mitigate the consequences of other transients and accidents.

In MODES 1, 2, and 3, an SIS train consists of an SI pump, the piping, instruments, and controls to ensure an OPERABLE flow path capable of taking suction from the IRWST on an SIAS from PPS or DPS.

During an event requiring SIS actuation, a flow path is provided to ensure an abundant supply of water from the IRWST to the RCS via the SI pumps and their respective supply lines to each of the four direct vessel injection nozzles. In the long term, flow paths may be switched to supply part of its flow to the RCS hot legs via the SCS suction nozzles on two of the trains.

The flow path for each train must maintain its designed independence to ensure that no single failure can prevent delivery of the minimum required flow rate.

APPLICABILITY

In MODES 1, 2, and 3 the SIS 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 also does provide for reduced cooling requirements in the lower MODES. Surveillance requirements for SI pump testing are based on the limiting safety analyses. Surveillance requirements for SI pump performance are specified to ensure that head/flow characteristics, as measured at design conditions, are within the tolerances allowed in developing the SI delivery curves over the operating range from shutoff head to runout flow.

BASES

APPLICABILITY (continued)

The SIS functional requirements for MODES 4, 5, and 6 are described in LCO 3.5.3.

ACTIONS

A.1

If two[1] or less trains are inoperable, the inoperable components must be returned to OPERABLE status within 72 hours. The 72-hour Completion Time is based on an NRC study (Reference 4) using a reliability evaluation and is a reasonable amount of time to effect many repairs.

An SIS 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 (except as allowed by their respective LCOs).

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 SIS 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 SIS. 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 diesel generator can disable one SIS train until power is restored. It is assumed that flow from the second SI pump is discharged through the break. Analysis has shown that flow from one SI pump is sufficient to keep the core covered for a break the size of a DVI nozzle which is the limiting SBLOCA. Hence, continued operation for 72 hours is justified.

(1) The two injection lines corresponding to the two inoperable trains are diagonal in reactor vessel (i.e., SI train# 1/3 or 2/4).

BASES

ACTIONS (continued)

B.1 and B.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 followed by placing the plant 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 in an orderly manner and without challenging unit systems.

C.1

If two[1] or more than SIS trains are inoperable, the unit is in a condition outside the accident analysis. Therefore, LCO 3.0.3 must be entered immediately.

SURVEILLANCE REQUIREMENTS

SR 3.5.2.1

Verification of proper valve position ensures the flow path from the SIS pumps to the RCS is maintained. Misalignment of these valves could render the associated SIS train inoperable. Securing these valves in position by locking after positioning them in the correct position ensures that the valves cannot be inadvertently misaligned or change position as the result of an improper operation (e.g., unauthorized, inadvertent). A 12-hour Frequency is considered reasonable in view of other administrative controls ensuring that a mispositioned valve is an unlikely possibility.

(1) The two injection lines corresponded to the two inoperable trains are not diagonal in reactor vessel (i.e., SI train# 1/2, 1/4, 2/3 or 3/4).

SURVEILLANCE REQUIREMENTS (continued)

SR 3.5.2.2

Verifying the correct alignment for manual, power operated, and automatic valves in the SIS flow paths provides assurance that the proper flow paths will exist for SIS operation. This SR does not apply to valves which are locked, sealed or otherwise secured in position since these were verified to be in the correct position prior to locking, sealing or securing. A valve which receives an actuation signal is allowed to be in a non-accident 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, an improper valve position would only affect a single train, and the probability of an event requiring SIS actuation during this time period is low. This Frequency has been shown to be acceptable through operating experience.

SR 3.5.2.3

With the exception of systems in operation, the SIS pumps are normally in a standby, non-operating condition. As such, flow path piping has the potential to develop voids and pockets of entrained gases. Maintaining the piping from the SIS pumps to the RCS full of water ensures that the system will perform properly, injecting its full capacity into the RCS upon demand. Water source comes from the IRWST and safety injection filling tanks (SIFTs). This will also prevent water hammer, pump cavitation, and pumping of non-condensible gas (e.g., air, nitrogen, hydrogen) into the reactor vessel during shutdown cooling or following an SIAS from PPS or DPS. The 31-day Frequency is based on the low probability of an event requiring SIS actuation during this time, the gradual nature of gas accumulation in the SIS piping, and the adequacy of procedural controls governing system operation.

SURVEILLANCE REQUIREMENTS (continued)

SR 3.5.2.4

Periodic Surveillance testing of SIS pumps to detect gross degradation caused by impeller structural damage or other hydraulic component problems is required by Section XI of 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, which encompasses the ASME OM Code. Section XI of the ASME Code provides the activities and Frequencies necessary to satisfy the requirements.

SR 3.5.2.5

Discharge head at design flow is a normal test of SI pump performance required by the ASME OM Code. The Frequency for such tests is a Code requirement. Such inservice inspections detect component degradation and incipient failures.

SR 3.5.2.6 and SR 3.5.2.7

These SRs demonstrate each automatic SIS valve actuates to its required position on an actual or simulated safety injection actuation signal (SIAS) from PPS or DPS and that each SIS Pump starts on receipt of an actual or simulated SIAS from PPS or DPS. 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.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.5.2.8

Periodic inspections of the IRWST, holdup volume tank, IRWST strainers, and HVT trash racks ensure equipment is unrestricted and 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. DCD Tier 2, Chapter 6.
4. NRC Memorandum R. L. Bayer to V. Stello, Jr., “Recommended Interim Revisions to LCOs for ECCS Components,” December 1, 1975.

B 3.5 EMERGENCY CORE COOLING SYSTEM (ECCS)

B 3.5.3 Safety Injection System (SIS) – Shutdown

BASES

BACKGROUND

The Background section for Bases B 3.5.2, "Safety Injection System (SIS) – Operating," is applicable to these Bases with the following modifications:

In MODES 4, 5, and 6 with RCS level less than 39.7 m (130 ft), the decay heat generation and RCS blowdown rates are such that a single SI pump is capable of providing the core cooling function in the event of a loss of coolant accident (LOCA). Also, a zero power steam line break will have negligible consequences with respect to a reactivity transient.

APPLICABLE SAFETY ANALYSES

The Applicable Safety Analysis section of Bases 3.5.2 is applicable to this Bases. SIS – Shutdown satisfies LCO Selection Criterion 3.

Due to the stable conditions associated with operation in MODES 4, 5, and 6 with RCS level less than 39.7 m (130 ft), and the reduced probability of a design basis accident (DBA), the SIS operational requirements are reduced. Included in these reductions is that certain automatic safety injection (SI) actuation signals are not available. In these MODES, sufficient time exists for manual actuation of the required SIS to mitigate the consequences of an DBA.

Only two trains of SIS are required for MODES 4, 5 and 6 with RCS level less than 39.7 m (130 ft). Protection against single failure is not relied on for these MODES of operation.

LCO

During an event requiring SIS actuation, a flow path is required to supply water from the IRWST to the RCS via each SI pump to one of the four direct vessel injection (DVI) nozzles. In the long term, this flow path may be switched take its supply from the IRWST and to deliver its flow to the RCS hot leg and DVI nozzle.

Two operable SI trains ensure at least one pump is capable of adequate flow to the core in the event of a LOCA.

BASES

APPLICABILITY

In MODES 1, 2 and 3, the OPERABILITY requirements for SIS are covered by LCO 3.5.2.

In MODES 4, 5, and 6 with RCS level less than 39.7 m (130 ft), a loss of coolant resulting from a DVI line break requires two SI trains to be operable to ensure that if a LOCA disables one train an alternate SIS train is available. The requirement of having two OPERABLE SI trains is acceptable without single failure consideration on the basis of the stable reactivity condition and the limited core cooling requirements.

ACTIONS

A.1

With only one SI pump OPERABLE, the unit is not prepared to respond to a LOCA. The 1-hour Completion Time to restore at least two SIS trains to OPERABLE status ensures prompt action is taken to restore the required cooling capacity.

B.1.1, B.1.2, and B.2

The plant must be placed in a condition in which the LCO does not apply if SIS cannot be returned to OPERABLE status within the associated completion time. An RCS level of greater than 39.7m (130 ft) (the top of the reactor vessel flange) will provide a minimum water inventory in the event of a LOCA. In addition, the reduction of RCS cold leg temperature to less than 57.2 °C (135°F) will provide a reduction in clad temperature. The 24-hour Completion Time limits the time the plant is subject to conditions where the LCO is applicable.

SURVEILLANCE REQUIREMENTS

SR 3.5.3.1

The applicable Surveillance descriptions from Bases LCO 3.5.2 apply.

REFERENCES

The applicable references from bases 3.5.2 apply.

B 3.5 EMERGENCY CORE COOLING SYSTEM (ECCS)

B 3.5.4 In-Containment Refueling Water Storage Tank (IRWST)

BASES

BACKGROUND

The In-containment refueling water storage tank (IRWST) supports the safety injection system (SIS) and the containment spray system (CSS) as a source of borated water for engineered safety feature (ESF) pump operation.

The IRWST supplies four trains of SIS with borated water. Each SIS train has a separate suction line. The IRWST also supplies two containment spray pumps. Use of a single IRWST to supply four trains of SIS and two divisions of containment spray is acceptable since the IRWST is a passive component, and passive failures are not assumed to occur coincidently with a design basis event.

The shutdown cooling (SC) pump is interchangeable with the containment spray pump of the same division (i.e., the shutdown cooling pump can be used as a backup to the containment spray pump of the same division and vice versa). The shutdown cooling pump can take suction from the IRWST when it is used as a backup for the containment spray pump.

The safety injection (SI), SC, and containment spray (CS) pumps are provided with recirculation lines that ensure each pump can maintain minimum flow requirements when operating at shutoff head conditions. The SI pump recirculation lines discharge back to the IRWST. The SC and CS pumps have individual recirculation loops with heat exchangers which discharge back to the pump suction.

This LCO ensures that the IRWST contains sufficient borated water to support the SIS during a LOCA, ensures the reactor remains subcritical following a LOCA, ensures sufficient scrub of radioactive iodines and particulates in the containment atmosphere and dilution of radionuclide in water for limiting offsite dose, and ensures that the assumptions used in the safety analysis for containment net free volume are maintained. Insufficient water inventory in the IRWST could result in insufficient cooling capacity of the SIS and CSS, higher risk on core degradation and containment integrity, and higher offsite doses following a LOCA.

Improper boron concentrations could result in a reduction of SHUTDOWN MARGIN 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.

BACKGROUND (continued)

Storage capacity of the IRWST is based on operational and safety analysis requirements. The minimum LCO volume is based upon SIS and CSS requirements. The maximum LCO volume is determined such that the water surface is lower than the bottom of the reactor vessel, even if the IRWST water is flooded in the reactor cavity due to an inadvertent operation of the cavity flooding system during normal operation. The IRWST temperature requirements are based on an inadvertent containment spray actuation.

The IRWST supplies the CSS, covered in LCO 3.6.6, “Containment Spray System," and the SIS, covered in LCOs 3.5.2, “Safety Injection System (SIS) – Operating,” and 3.5.3, “Safety Injection System (SIS) – Shutdown,” with sufficient borated water to meet GDC 35 (Reference 1).

APPLICABLE SAFETY ANALYSES

During design bases accident conditions the IRWST provides a source of borated water to the SI pumps and CS pumps or SC pumps. As such, it supports containment cooling and depressurization, core cooling and maintaining cooling water inventory, RCS depressurization using feed and bleed methods, and keeping reactor shutdown margin. The design basis transients and applicable safety analyses concerning each of these systems are discussed in the applicable safety analyses sections of Bases for LCOs 3.5.2, 3.5.3, and 3.6.6. These analyses are used to assess changes to the IRWST in order to evaluate their effects in relation to the acceptance limits.

The minimum volume in the IRWST of 2,373 m^3 (627,000 gal) is required for continuous SIS and CSS operation and used for safety analyses. The maximum volume of IRWST of 2,541 m^3 (671,162 gal) is determined such that the water surface is lower than the bottom of the reactor vessel, even if the IRWST water is flooded into the reactor cavity due to an inadvertent operation of the cavity flooding system during normal operation. A free space of 752.8 m^3 (26,584 ft^3) in the IRWST is assumed for a safety analysis of hydrogen concentration in IRWST. This free volume is guaranteed if the IRWST water volume is less than the maximum volume in the IRWST of 2,541 m^3 (671,162 gal).

APPLICABLE SAFETY ANALYSES (continued)

The LOCA dose analyses assumes a volume of at least (2,373 m^3 [627,000 gal]) for dilution of radionuclide in water. The 4,000 ppm limit for minimum boron concentration was established to ensure that, following a LOCA with a minimum IRWST level, the reactor will remain subcritical in the cold condition following mixing of the IRWST 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 life.

The maximum boron limit of 4,400 ppm in the IRWST 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, boron precipitation will occur in the core. Post-LOCA emergency procedure directs the operator to establish simultaneous hot leg/DVI nozzle injection to prevent this condition by a forced flow through the core regardless of break location.

This procedure is based upon the minimum time in which precipitation could occur, assuming the maximum LCO limit of the IRWST boron concentration. Boron concentrations in the IRWST in excess of the limit could result in precipitation earlier than assumed in the analysis.

The safety analyses assumes the minimum allowed IRWST water temperature is 10 °C (50 °F) and the maximum temperature of the IRWST is 49 °C (120 °F).

The IRWST satisfies LCO SELECTION CRITERION 3.

LCO

The IRWST 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. The IRWST ensures the reactor remains subcritical following a DBA.

To be considered OPERABLE, the IRWST must meet the limits established in the SR for water volume, boron concentration and temperature.

BASES

APPLICABILITY

In MODES 1, 2, 3 and 4, the IRWST OPERABILITY requirements are dictated by the SIS and CSS OPERABILITY requirements. Since both the SIS and CSS must be OPERABLE in MODES 1, 2, 3 and 4, the IRWST must be OPERABLE to support these systems.

In MODES 5 and MODE 6 with RCS level less than 39.7 m (130 ft), the IRWST OPERABILITY requirements are dictated by the SIS. The requirements of SIS are specified in LCO 3.5.3. Two trains of SIS, one in each division, are required in these MODES, therefore the IRWST must be OPERABLE to support the SIS.

MODE 6 considers a loss of decay heat removal (DHR) resulting from a break in the bottom of the hot leg or a lower head instrument line (2.8 cm^2 [0.003 ft^2]). If the reactor coolant water level is above the reactor vessel flange (greater than 39.7 m [130 ft]), the low power shutdown risk is negligible because sufficient water inventory in refueling pool is available.

ACTIONS

A.1

With IRWST boron concentration or borated water temperature not within limits, they must be returned to within limits within 8 hours. In this condition neither the SIS nor the CSS can perform its 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 IRWST boron concentration or temperature 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 IRWST borated water volume not within limits, it must be returned to within limits within 1 hour. In this condition neither the SIS nor the CSS can perform its design function; therefore, prompt action must be taken to restore the tank to OPERABLE status or to place the plant in a MODE in which these systems are not required. The Completion Time of 1 hour to restore the IRWST to OPERABLE is based on this condition simultaneously affecting multiple trains.

ACTIONS (continued)

C.1, and C.2

If the IRWST cannot be returned to OPERABLE status within the associated Completion Time, the plant must be brought to a condition 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 condition from full power and shutdown conditions in an orderly manner and without challenging plant systems.

D.1 and D.2

The plant must be placed in a condition in which the LCO does not apply if SIS cannot be returned to OPERABLE status within the associated Completion Time. An RCS level of greater than 39.7m (130 ft) (the top of the reactor vessel flange) will provide a minimum water inventory in the event of a LOCA. In case that the reactor water level is below the reactor vessel flange with head off in MODE 6, one safety injection pump is required immediately after loss of coolant accident at the low power shutdown condition according to the shutdown LOCA safety analysis. If the reactor coolant water level is above the reactor vessel flange with head off in MODE 6, the low power shutdown risk is negligible because sufficient water inventory in refueling pool is available.

Therefore, the reactor flange water level above the reactor vessel flange with head off in MODE 6 does not require one safety injection pump after loss of coolant accident at low power shutdown risk. In addition, if RCS water level is below the flange of the reactor vessel, there is a potential of evaporation of the coolant. The reduction of RCS cold leg temperature to less than 57.2 °C (135°F) will provide a reduction in clad temperature. If RCS cold leg temperature reaches above 57.2 °C (135°F), there is a potential to evaporate. The 24-hour Completion Time limits the time the plant is subject to conditions where the LCO is applicable.

SURVEILLANCE REQUIREMENTS

SR 3.5.4.1

IRWST 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.

SR 3.5.4.2

The IRWST water volume must be maintained equal to or more than the required minimum value and equal to or less than the maximum value. IRWST water volume shall be verified every 7 days. Since the IRWST water volume is normally stable and 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

The boron concentration of the IRWST 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 IRWST pH is 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 IRWST volume is normally stable, a 7-day sampling Frequency is appropriate and has been shown through operating experience to be acceptable.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 35.
2. DCD Tier 2, Chapter 6.
3. DCD Tier 2, Chapter 15.

B 3.5 EMERGENCY CORE COOLING SYSTEM (ECCS)

B 3.5.5 Trisodium Phosphate (TSP)

BASES

BACKGROUND

The in-containment refueling water storage tank (IRWST) is the suction source for the Safety Injection (SI) pumps and containment spray (CS) pumps during short-term injection and long-term cooling MODES of post-accident operation. Reactor coolant blown out through a break and water sprayed by the CS pumps during a LOCA is collected in the holdup volume tank (HVT). The accumulated water in the HVT overflows back into the IRWST, thereby the IRWST is replenished. Trisodium phosphate dodecahydrate (TSP) is placed in the baskets mounted on the wall of the HVT so that it can be dissolved without any operator action. The dissolved TSP prevents the iodine, which is dissolved in the collected reactor cooling water and sprayed water, from evolving to the air. TSP also helps inhibit stress corrosion cracking (SCC) of austenitic stainless steel components in containment during the long-term cooling 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 HVT by containment sprays.

The emergency core cooling water is borated for reactivity control. This borated water causes the HVT 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 level of airborne iodine. The increased level of airborne iodine increases the radiological releases and consequences due to containment leakage following an accident.

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 stress corrosion cracking (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.

BACKGROUND (continued)

Maintaining the pH of the solution circulated by SI and CS pumps 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 occurrences of SCC of austenitic stainless steel components in containment. Reducing SCC reduces the probability of failure of components.

TSP is employed as a passive form of pH control for post LOCA containment spray and core cooling water. TSP baskets are mounted on the wall of the HVT for TSP to be dissolved with the released reactor coolant water and containment sprayed water after a LOCA.

Recirculation of the water for core cooling and containment spray then provides mixing to achieve a uniform solution pH. The dodecahydrate form of TSP is used because of the humidity inside containment 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 recirculated water pH being greater than or equal to 7.0. The radionuclide releases from the containment atmosphere and the consequences of a LOCA would be increased if the pH of the recirculated water were not adjusted to 7.0 or above.

TSP satisfies LCO SELECTION CRITERION 3.

BASES

LCO

The TSP is required to adjust the pH of the recirculated water to greater than 7.0 after a LOCA. A pH greater than 7.0 is necessary to prevent significant amounts of iodine released from fuel failures and dissolved in the recirculated water from converting to a volatile form and evolving into the containment atmosphere. Higher levels of airborne iodine in containment could increase the release of radionuclides and the consequences of the accident. A pH greater than 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 HVT after a large break LOCA. The minimum required volume is the volume of TSP that will achieve a solution pH of greater than or equal to 7.0 when taking into consideration the maximum possible water volume and the minimum possible pH. The amount of TSP needed in the containment 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 due to humidity inside containment, 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.

APPICABILITY

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 HVT is not within limit, action must be taken to restore the TSP to within limit. During plant operation, the HVT is not accessible and corrective ACTIONS 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 variables.

BASES

ACTIONS (continued)

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 chosen to allow reaching the specified conditions from full power in an orderly manner without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.5.5.1

The stainless steel baskets, which are mounted on the walls of the HVT, have a solid top and bottom with mesh sides to permit submergence of the TSP. The elevation of the baskets is above the normal operating water level in the HVT and below the IRWST spillway. Access is provided to the baskets for inspection and sampling.

Periodic identification of the volume of TSP in the containment must be performed due to the possibility of leaking valves and components inside containment that could cause the dissolution of TSP during normal operation. It is required to determine visually with a Frequency of 18 months that a minimum of 29.5 m^3 (1,042 ft^3) is contained in the TSP baskets. This requirement ensures that there is a sufficient volume of TSP to maintain the pH of the post LOCA solution above 7.0.

The Surveillance Frequency is determined to be 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.

SR 3.5.5.2

Testing must be performed to ensure the solubility and pH control ability of the TSP is maintained after exposure to the containment environment. A representative sample of 30.3 g of TSP from one of the baskets in containment is submerged in borated water of 3.8±0.19 liters (1.0±0.05 gallon) at the temperature of 25±5 °C (77±9 °F). Without agitation, the solution pH should be raised to 7.0 or above within 4 hours.

SURVEILLANCE REQUIREMENTS (continued)

The representative sample weight is based on the minimum required TSP weight of 26,471 kg (58,358 lb), which corresponds to a minimum volume of 29.5 m^3 (1,042 ft^3) at manufactured density, normalized to buffer a 3.8 liters (1.0 gallon) sample. The boron concentration of the test water is representative of the maximum possible boron concentration corresponding to the maximum possible post-LOCA recirculation water 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. Since the TSP and boated water would mix in the HVT following a LOCA better than the test without agitation, it takes considerably less time to achieve the required pH actually.

This would ensure compliance with the SRP requirement of a pH greater than or equal to 7.0 by the onset of recirculation after a LOCA.

The Surveillance Frequency is determined to be 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.

REFERENCE None.

B 3.6 CONTAINMENT SYSTEMS

B 3.6.1 Containment

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 could 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 could 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 using 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 B (Reference 4), 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.

   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.”

BACKGROUND (continued)

b. Each airlock is OPERABLE except as provided in LCO 3.6.2, "Containment Airlocks."

c. All equipment hatches are closed.

d. The pressurized sealing mechanism associated with a penetration, except as provided in LCO 3.6.1, 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 which result in a release of radioactive material within containment are a loss of coolant accident (LOCA), a main steam line break(MSLB), a main feedwater line break (MFLB), and a control element assembly (CEA) ejection accident (Reference 2).

In the analysis of each of these accidents, it is assumed that the containment is OPERABLE at event initiation such that the majority of the release of fission products to the environment is controlled by the rate of containment leakage. In addition, for the above accidents, it is assumed that the containment low volume purge is operating at event initiation. Isolation of the purge will be automatic or manual depending upon the pressure transient associated with the analyzed accident.

The containment was designed with an allowable leakage rate of 0.1 % of the containment volume per day (Reference 3). This leakage rate, used in the evaluation of offsite doses resulting from accidents, is defined in 10 CFR 50, Appendix J, Option B, as La: the maximum allowable containment leakage rate at the calculated maximum peak containment pressure (Pa) following a DBA. The calculated maximum peak containment pressure 3.66 kg/cm^2G (52.09 psig) was obtained from a double ended discharge leg slot break (DEDLSB) with maximum ECCS flow. The containment internal design pressure is (4.218 kg/cm^2G [60 psig]). The allowable leakage rate represented by La forms the basis for the acceptance criteria imposed on all containment leak rate testing.

Satisfactory leak test results are a requirement for the establishment of containment OPERABILITY.

APPLICABLE SAFETY ANALYSES (continued)

The acceptance criteria applied to accidental releases of radioactive material to the environment are given in terms of total effective dose (TED) received by a member of the general public who remains at the exclusion area boundary for any two hours period following onset of the postulated fission product release. The limit established in Reference 1 is 0.25 Sv total effective dose.

The containment satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii)

LCO

Containment OPERABILITY is maintained by limiting leakage to less than or equal to 1.0 La, 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 airlocks (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 La.

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 MODES 6 are addressed in LCO 3.9.3, “Containment Penetrations.”

BASES

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 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 where containment is inoperable is minimal.

B.1 and B.2

If containment cannot be restored to OPERABLE status in the associated Completion Time, the plant must be placed in 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 containment OPERABLE requires compliance with the visual examinations and leakage rate test requirements of Containment Leakage Rate Testing Program. The containment concrete visual examinations may be performed during either power operation (e.g., 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 airlock and purge valve with resilient seal specific leakage limits specified in LCOs 3.6.2 and 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 limits to be exceeded. As-left leakage prior to the startup after performing a required Containment Leakage Rate Testing Program is required to be less than or equal to 0.6 La for combined Type B and C leakage and less than or equal to 0.75 La for option B for overall Type A leakage.

SURVEILLANCE REQUIREMENTS (continued)

At all other times between required leakage rate tests, the acceptance criteria is based on an overall Type A leakage limit of less than or equal to 1.0 L_a. At less than or equal to 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.

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 consistent with the ASME Code, Section XI, Subsection IWL (Reference 5) and applicable addenda as required by 10 CFR 50.55a.

REFERENCES

1. 10 CFR 50.34.
2. DCD Tier 2, Chapter 15.
3. DCD Tier 2, Section 6.2.
4. 10 CFR 50, Appendix J, Option B.
5. ASME Section XI, Subsection IWL.

B 3.6 CONTAINMENT SYSTEMS

B 3.6.2 Containment Airlocks

BASES

BACKGROUND

Two containment airlocks form part of the containment pressure boundary and provide a means for personnel access during all MODES of operation.

Each airlock is nominally a right circular cylinder 3.05 m (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 to remain open for extended periods when frequent containment entry is necessary. Each airlock door has been designed and tested to certify its ability to withstand a pressure in excess of the maximum expected pressure following a 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 ensure a leak tight seal, the airlock design uses pressure seated doors (i.e., an increase in containment internal pressure results in increased sealing force on each door).

Each air personnel lock is provided with limit switches on both doors that provide main control room (MCR) indication of door position. Additionally, MCR indication is provided to alert the operator whenever an airlock door interlock mechanism is defeated.

The containment airlocks form part of the containment pressure boundary. As such, airlock integrity and leak-tightness is essential for maintaining the containment leakage rate within limit in the event of a DBA. Not maintaining airlock integrity or leak-tightness could result in a leakage rate in excess of that assumed in the unit safety analysis.

BASES

APPLICABLE SAFETY ANALYSES

For atmospheric containment the DBAs that result in a release of radioactive material within containment are a LOCA, a main steam line break (MSLB), a main feedwater line break (MFLB), and a CEA ejection accident (Reference 2). In the analysis of each of these accidents, it is assumed that containment is OPERABLE at event initiation, 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 0.1 % of containment volume per day (Reference 3). This leakage rate is defined in 10 CFR 50, Appendix J, Option A, as L_a: the maximum allowable containment leakage rate at the calculated maximum peak containment pressure (P_a) of 3.66 kg/cm^{2}G (52.09 psig), which results from the limiting DBA (a DEDLSB with maximum ECCS flow) (Reference 3). This allowable leakage rate forms the basis for the acceptance criteria imposed on the SR associated with the airlock.

The containment airlocks satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

Each containment airlock forms part of the containment pressure boundary.
As part of containment, the airlock safety function is related to control of the containment leakage rate resulting from a DBA. Thus, each airlock's structural integrity and leak tightness is essential to the successful mitigation of such an event.

Two airlocks are required to be OPERABLE. For the airlock to be considered OPERABLE, the airlock interlock mechanism must be OPERABLE, the airlock must be in compliance with the Type B airlock leakage test, and both airlock doors must be OPERABLE. The interlock allows only one airlock door of an airlock 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 airlock is sufficient to provide a leak tight barrier following postulated events. Nevertheless, both doors are kept closed when the airlock is not being used for normal entry into and 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 airlocks are not required in MODE 5 to prevent leakage of radioactive material from containment. The requirements for the containment airlocks 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 airlock component. If the outer door is inoperable, then it can be easily accessed for most repairs. It is preferred that the airlock be accessed from inside containment by entering through the other OPERABLE airlock. 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 airlock through the OPERABLE door, which means there is a short time during which the containment boundary is not intact(during access through the outer 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 airlock.

A second Note has been added to provide clarification that, for this LCO, separate Condition entry is allowed for each airlock. This is acceptable, since the Required Actions for each Condition provide appropriate compensatory action for each inoperable airlock. Complying with the Required Actions may allow for continued operation, and a subsequent inoperable airlock 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.

ACTIONS (continued)

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

With one airlock door inoperable in one or more containment airlocks, the OPERABLE door must be verified closed (Required Action A.1) in each affected containment airlock. This ensures that a leak tight containment barrier is maintained by the use of an OPERABLE airlock door. This action must be completed within 1 hours. 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.

In addition, the affected airlock penetration must be isolated by locking closed an OPERABLE airlock door within the 24-hour Completion Time. The 24-hour Completion Time is considered reasonable for locking the OPERABLE airlock door considering the OPERABLE door of the affected airlock is being maintained closed.

Required Action A.3 verifies that an airlock with an inoperable door has been isolated by the use of a locked and closed OPERABLE airlock 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 airlock 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 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 airlock are inoperable. With both doors in the same airlock 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 airlock for entry and exit for 7 days under administrative controls if both airlocks have an inoperable door.

ACTIONS (continued)

This 7-day restriction begins when the second airlock 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 airlock, 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.

B.1, B.2, and B.3

With an airlock door interlock mechanism inoperable in one or more airlocks, 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 airlock are inoperable. With both doors in the same airlock 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 airlock 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 airlock 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.

ACTIONS (continued)

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

With one or more airlocks 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 per LCO 3.6.1, “Containment,” using current airlock test results. An evaluation is acceptable since it is overly conservative to immediately declare the containment inoperable if both doors in an airlock have failed a seal test or if the overall airlock 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 airlock 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 airlock 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.

Additionally, the affected airlocks must be restored to OPERABLE status within the 24-hour Completion Time. The specified time period is considered reasonable for restoring an inoperable airlock to OPERABLE status, assuming that at least one door is maintained closed in each affected airlock.

D.1 and D.2

If the inoperable airlock cannot be restored to OPERABLE status within the required Completion Time, the plant must be placed in 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 airlocks OPERABLE requires compliance with the leakage rate test requirements of Containment Leakage Rate Testing Program (Reference 1). This SR reflects the leakage rate testing requirements with regard to airlock leakage (Type B leakage tests). The acceptance criteria were established during initial airlock and containment OPERABILITY testing. The periodic testing requirements verify that the airlock leakage does not exceed the allowed fraction of the overall containment leakage rate. The Frequency is required by Containment Leakage Rate Testing Program. Thus, SR 3.0.2 (which allows Frequency extensions) does not apply.

The SR has been modified by two Notes. Note 1 states that an inoperable airlock door does not invalidate the previous successful performance of the overall airlock leakage test. This is considered reasonable since either airlock door is capable of providing a fission product barrier in the event of a DBA. Note 2 requires the results to be evaluated against the acceptance criteria of SR 3.6.1.1. This ensures that airlock leakage is properly accounted for in determining the overall containment leakage rate.

SR 3.6.2.2

The airlock door interlock is designed to prevent simultaneous opening of both doors in a single airlock. Since both the inner and outer doors of an airlock 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 airlock 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 inner and outer door 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 upon entering containment but is not required more frequently than every 24 months.

BASES

SURVEILLANCE REQUIREMENTS (continued)

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 B.
2. DCD Tier 2, Chapter 15.
3. DCD Tier 2, Section 6.2.

B 3.6 CONTAINMENT SYSTEMS

B 3.6.3 Containment Isolation Valves

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, deactivated 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 accident 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 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 containment function assumed in the accident analysis will be maintained.

BACKGROUND (continued)

Containment 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: high volume purge valves and low volume purge valves. The containment high volume purge system and low volume purge system purge the containment atmosphere to the unit vent. The high volume purge and low volume purge supply and exhaust lines are each supplied with inside and outside containment isolation valves. The high volume purge valves are designed for purging the containment atmosphere to the unit stack while introducing filtered make up from the outside to provide adequate ventilation for personnel comfort when the unit is shutdown during refueling operations and maintenance. The low volume purge system is a pressure relief system that is used to relieve containment pressure during startup or shutdown. These containment isolation valves (with the exception of check valves used as containment isolation valves) are operated manually from the MCR. The valves will close automatically upon receipt of a Containment purge isolation signal. Air-operated valves fail closed upon a loss of instrument air.

Because of their large size, the high volume purge containment isolation valves are not qualified for automatic closure from their open position under DBA conditions. Therefore, the high volume purge containment isolation valves (supply and exhaust) are normally maintained closed in MODES 1, 2, 3, and 4 to ensure the containment boundary is maintained.

Open high volume purge valves or failure of the low volume purge 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 requirements related to minimizing the loss of reactor coolant inventory and establishing the containment boundary resulting from major accidents. As part of the containment boundary, containment isolation valve and containment purge valve OPERABILITY support leak tightness of the containment. Therefore, the safety analysis of any event requiring isolation of containment is applicable to this LCO.

APPLICABLE SAFETY ANALYSES (continued)

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), a main feedwater line break (MFLB), or a control element assembly (CEA) 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 leakage paths to the environment through containment isolation valves (including containment purge valves) are minimized. The safety analysis assumes that the high volume 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 leak 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.

The single failure criteria required to be imposed in the conduct of unit safety analyses was considered in the 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 high volume purge valves could be unable to close in the environment following a LOCA. Therefore, each of the high volume purge valves is required to remain sealed closed during MODES 1, 2, 3, and 4. In this case, the single failure criteria remain 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 the system is operated in accordance with the subject LCO.

The low volume purge 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).

BASES

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. The valves covered by this LCO are listed with their associated stroke times in Chapter 6 (Reference 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 Chapter 6 (Reference 1).

Purge valves with resilient seals 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 function 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 MODES are addressed in LCO 3.9.3, “Containment Penetrations”.

ACTIONS

The ACTIONS are modified by a Note allowing penetration flow paths, except for 1219.2 mm (48 in) 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 in continuous communication with the MCR. 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.

ACTIONS (continued)

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.

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 except for purge valve 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 A.1, the valve 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.

For affected penetrations which 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 path 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 valve 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.

ACTIONS (continued)

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 A has been modified by a Note indicating that this Condition is only applicable to those penetration flow paths with two containment isolation valves. For penetration flow paths with only one containment isolation valve and a closed system, Condition C provides appropriate actions.

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. There, the probability of misalignment of these devices, once they have been verified to be in the proper position, is small.

B.1

With two containment isolation valves in one or more penetration flow paths inoperable except for purge valve 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 B.1, the affected penetration must be verified to be isolated on a periodic basis per Required Action A.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.

ACTIONS (continued)

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 B is modified by a Note indicating this Condition is only applicable to penetration flow paths with two containment isolation valves. Condition A of this LCO addresses the condition of one containment isolation valve inoperable in this type of penetration flow path.

C.1 and C.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 C.1 must be completed within the 4 hour Completion Time. 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 penetration is isolated in accordance with Required Action C.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 C 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. This Note is necessary since this Condition is written to specifically address those penetration flow paths in a closed system.

ACTIONS (continued)

Required Action C.2 is modified by a Note that 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. Therefore, the probability of misalignment of these valves, once they have been verified to be in the proper position, is small.

D.1, D.2, and D.3

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 deactivated automatic valve with resilient seals, a closed manual valve with resilient seals, or a blind flange. A purge valve with resilient seals used to satisfy Required Action D.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 D.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, through a system walkdown, that those isolation devices outside 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.

BASES

ACTIONS (continued)

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.

For the containment purge valve with resilient seal that is isolated in accordance with Required Action D.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 Generic Issue B-20 (Reference 2). 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.

E.1 and E.2

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.

SURVEILLANCE REQUIREMENTS

SR 3.6.3.1

Each 1219.2 mm (48 in) 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 prevent offsite dose limits. Therefore, these valves are required to be in the sealed closed position during MODES 1, 2, 3, and 4.

SURVEILLANCE REQUIREMENTS (continued)

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 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 Generic Item B-24, related to containment purge valve use during plant operations (Reference 3). This SR is not required to be met while in condition D of this LCO. This is reasonable since the penetration flow path would be isolated.

SR 3.6.3.2

This SR ensures the 203.2 mm (8 in) purge valves are closed as required, or, if open, open for an allowable reason. 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, and air quality considerations for personnel entry, and for Surveillance that require the valves to be open. The 203.2 mm (8 in) purge 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 under 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 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, through a system walkdown, that those containment isolation valves outside containment and capable of being mispositioned are in the correct 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.

SURVEILLANCE REQUIREMENTS (continued)

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, and 4 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 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 and flanges 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 the primary containment is inerted and 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.

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 Frequency of this SR is in accordance with the Inservice Testing Program.

BASES

SURVEILLANCE REQUIREMENTS (continued)

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 B (Reference 4), 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 Generic Issue B-20 (Reference 2).

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.

REFERENCES

1. DCD Tier 2, Chapter 6.

2. Generic Issue B-20.

3. Generic Issue B-24.

4. 10 CFR 50, Appendix J, Option B.

B 3.6 CONTAINMENT SYSTEMS

B 3.6.4 Containment Pressure

BASES

BACKGROUND

The containment structure serves to contain radioactive material that could be released from the reactor core following a design basis accident (DBA), such that offsite radiation exposures are maintained within the requirement of 10 CFR 50.34 (Reference 1). 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 which is monitored and controlled during MODES 1 through 4. 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), a loss of containment integrity could result. Loss of containment integrity could cause site boundary doses, due to a DBA, to exceed values given in Reference 3.

APPLICABLE SAFETY ANALYSES

The limits for containment pressure ensure that operation is maintained within the design and accident analysis bases for containment. The accident analyses and evaluations include both LOCAs and MSLBs to determine the maximum peak containment pressure (P_a). A double-ended discharge leg slot break with maximum safety injection (SI) flow results in the highest calculated internal containment pressure of 3.66 kg/cm^{2}G (52.09 psig). This is below the internal design pressure of 4.218 kg/cm^{2}G (60 psig), also the LOCA event bounds all of the MSLB events from the viewpoint of the containment peak pressure.

The initial pressure value used to calculate the containment peak pressure to LOCA is 0.1 kg/cm^{2}G (1.42 psig). The containment is also designed for a minimum internal pressure which is less than the containment external pressure by 0.281 kg/cm^2 (4.0 psi) to withstand the resultant pressure drop from accidental actuation of the containment spray system.

BASES

APPLICABLE SAFETY ANALYSES (continued)

The minimum containment internal pressure which would occur as a result of an inadvertent actuation of the containment spray system is -0.25 kg/cm^{2}G (-3.54 psig), starting with an initial pressure of -0.037 kg/cm^{2}G (-0.52 psig).

Containment pressure satisfies LCO SELECTION CRITERION 2.

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 a DBA are reduced due to the pressure and temperature limitations of these MODES.

ACTIONS

A.1

When containment pressure is not within the limits of the LCO, containment pressure must be restored 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 the containment be restored to OPERABLE status within 1 hour.

BASES

ACTIONS (continued)

B.1 and B.2

If containment pressure cannot be restored within limits within the required Completion Time, the plant must be placed in a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within six 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 3.6.4.1

Verifying containment pressure is within limits ensures that 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 containment pressure variations and pressure instrument drift during the applicable MODES, and the low probability of a DBA occurring between surveillances. Furthermore, the 12-hour Frequency is considered adequate in view of other indications in the MCR, including alarms, to alert the operator of an abnormal containment pressure condition.

REFERENCES

1. 10 CFR 50.34.

2. DCD Tier 2, Subsection 6.2.1.

B 3.6 CONTAINMENT SYSTEMS

B 3.6.5 Containment Air Temperature

BASES

BACKGROUND

The containment structure serves to contain radioactive material that could 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 limits are 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 system 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 could result in leakage greater than assumed in the accident analysis (Reference 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 analysis 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 include both LOCAs and MSLBs to determine the maximum peak containment pressures and temperatures. The worst case MSLB generates higher temperature than the worst case LOCA. Thus, the MSLB event bounds the LOCA event in a view of containment peak temperature.

BASES

APPLICABLE SAFETY ANALYSES (continued)

The initial pre-accident temperature inside containment was assumed to be 49 °C (120 °F) (Reference 2) and the calculated peak temperature is 170.3 °C (338.6 °F) at the event of MSLB (102 % power, MSIV single failure). However, this superheated condition does not influence the design of the containment, since it lasts only for a short period of time. Moreover, the superheated steam is condensed rapidly to saturated water after contact with the subcooled containment inner surface. The design temperature of structures within the containment including liner plate is determined to 143.3 °C (290 °F) based on saturated conditions at the steam partial pressure in containment.

The consequence of exceeding this design temperature could 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 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

With containment average air temperature not within the limit of the LCO, it must be restored within the 8 hours. The 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 limits within the required Completion Time, the plant must be brought to a MODE in which overall plant risk is minimized. To achieve this status, the plant must be brought to at least MODE 3 within six hours and to MODE 5 within 36 hours.

The allowable 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 the plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.6.5.1

Verifying the containment average air temperature is within the LCO limit ensures that containment operation remains within the limits assumed for the containment analyses. In order to determine the average 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).

REFERENCES

1. 10 CFR 50.34.

2. DCD Tier 2, Chapter 15.

B 3.6 CONTAINMENT SYSTEMS

B 3.6.6 Containment Spray System

BASES

BACKGROUND

The containment spray system (CSS) cools containment atmosphere to limit post-accident pressure and temperature 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), within regulatory limits. The CSS is designed to the requirements of 10 CFR 50, Appendix A, and GDC 39 through 43 (Reference 1).

The CSS is an engineered safety feature (ESF) system. It is designed to ensure that the heat removal capability required during the post-accident period can be attained. The CSS provides redundant methods to limit and maintain post-accident conditions to less than the containment design values.

In the event of a loss of coolant accident (LOCA) or a main steam line break (MSLB), the CSS sprays IRWST water into the containment atmosphere to reduce the post-accident energy and to remove fission product iodine. There are two redundant containment spray divisions.

Each division consists of one containment spray pump, one containment spray pump miniflow heat exchanger, one containment spray heat exchanger, one containment spray header and associated piping, valves, instrumentation and controls. The pumps and remotely operated valves can be operated from the main MCR.

A two-out-of-four pressurizer pressure low signal or a containment pressure high signal from the engineered safety features actuation system (ESFAS) generates a safety injection actuation signal (SIAS) which starts containment spray pumps.

A two out of four containment pressure high-high signal from the engineered safety features actuation system (ESFAS) generates a containment spray actuation signal (CSAS) which initiates containment spray operation. Upon receipt of a CSAS, the containment spray header isolation valve opens and the containment spray pump starts in each of the two redundant divisions.

BASES

BACKGROUND (continued)

The pumps take suction from the in-containment refueling water storage tank (IRWST) and discharge through the containment spray heat exchangers and the spray header isolation valves and to their respective spray nozzle headers, then into the containment atmosphere.

The CSS is capable of removing sufficient decay heat from the containment atmosphere following a DBA to maintain containment pressure and temperature within design limits.

The CSS protects the integrity of the containment by limiting the temperature and pressure following a DBA. Protection of adequate containment leaktightness prevents leakage of radioactive material from containment. Loss of adequate containment leaktightness could cause site boundary doses, due to a design bases LOCA, to exceed values given in Reference 3.

APPLICABLE SAFETY ANALYSES

The CSS limits the temperature and pressure following a DBA. The limiting DBAs considered relative to containment temperature and pressure are LOCA and MSLB. The 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 division of the CSS being rendered inoperable.

The accident analysis considers the worst case single active failure in the power supply which results in minimum containment cooling.

The analysis and evaluation show that under this scenario, the highest peak containment pressure is 3.66 kg/cm^{2}G (52.09 psig) during a LOCA, and actual temperature of the containment structure, remained below the maximum design temperature of 143.3 °C (290 °F). (See Bases B 3.6.4, “Containment Pressure,” and B 3.6.5, “Containment Air Temperature,” for a detailed discussion.)

The effect of an inadvertent containment spray actuation has been analyzed (Reference 5). An inadvertent containment spray actuation reduces the containment pressure to –0.25 kg/cm^{2}G (–3.54 psig) due to the sudden cooling effect in the interior of the air tight containment. Additional discussion is provided in Bases 3.6.4, “Containment Pressure.”

BASES

APPLICABLE SAFETY ANALYSES (continued)

The CSS actuation time in the containment analysis is based upon a response time associated with a containment high-high pressure signal to achieve full flow through the containment spray nozzles. The CSS total response time includes diesel generator startup (for loss of offsite power), load shedding and sequencing, containment spray pump startup, and spray line filling (Reference 2). The containment spray piping is full of water at least to the 26.213 m (86 ft) by difference in the static head between IRWST water level and containment spray piping. It minimizes the time required to fill the header.

The containment spray system satisfies LCO SELECTION CRITERION 3.

LCO

During a DBA, one containment spray division at least, is required to maintain the containment peak pressure and temperature below the design limits (Reference 2). One containment spray division 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 divisions must be OPERABLE. Therefore, in the event of an accident, the minimum requirements are met, even when the worst case single active failure occurs.

Each division of the CSS includes a containment spray pump, a containment spray heat exchanger, a containment spray pump mini-flow heat exchanger, containment spray headers, nozzles, valves, piping, instruments, and controls to ensure an OPERABLE flow path through which the IRWST borated water is supplied for containment spray upon an ESF actuation signal.

One or two shutdown cooling pumps can be aligned to meet the requirements of the associated containment spray pump in MODES 1, 2, and 3 when the shutdown cooling pumps are not required to be OPERABLE. In MODE 4 this is not allowed, since the shutdown cooling pumps should be in service for supporting the shutdown cooling function.

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 divisions.

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 is not required to be OPERABLE in MODES 5 and 6.

ACTIONS

A.1

With one containment spray division inoperable, the inoperable containment spray division must be restored to OPERABLE status within 72 hours. In this Condition, the remaining OPERABLE spray division is capable to perform the iodine removal and containment cooling functions. The Completion Time was determined to be 72 hours with taking into account the redundant heat removal capability, reasonable time for repairs, and the low probability of a DBA occurring during this period.

B.1 and B.2

If the inoperable containment spray division cannot be restored to OPERABLE status within the required Completion Time, the plant must be placed in 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 allowed Completion Time of 84 hours to reach MODE 5 allows additional time for the restoration of the containment spray division 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.

C.1

With two containment spray divisions inoperable, the unit is in a condition outside the accident analysis. Therefore, LCO 3.0.3 must be entered immediately.

SURVEILLANCE REQUIREMENTS

If the shutdown cooling pump is aligned to meet the requirements of the associated containment spray pump, then the Surveillance Requirements of this LCO must be applied to the shutdown cooling pump instead of the containment spray pump, as necessary.

SR 3.6.6.1

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 be available for CSS operation. This SR does not apply to valves which are locked, sealed, or otherwise secured in position since they were verified to be in the correct position prior to locking, sealing, or securing. This SR also does not apply to valves which cannot be inadvertently misaligned, such as check valves. A valve which receives an actuation signal is allowed to be in a non-accident position provided the valve will automatically reposition within the proper stroke time. This SR does not require any valve testing or manipulation. Rather, it involves verifying through a system walkdown that those valves outside containment are in the correct position.

SR 3.6.6.2

Verifying that each containment spray pump develops 13.99 kg/cm^2D (199.1 psid) of differential pressure at a flow rate of greater than or equal to 20,535.24 L/min (5,425 gpm) ensures that each containment spray pump performance has not degraded during the cycle. Flow and differential pressure are normal tests of centrifugal pump performance required by ASME OM Code (Reference 4).

Since the containment spray pumps cannot be tested with flow through the spray nozzles, they are tested on recirculation flow. The recirculation alignment is full flow to the IRWST. This test confirms pump performance. Such in-service inspections confirm component OPERABILITY, trend performance, and detect incipient failures by indicating abnormal performance. The frequency of this SR is in accordance with the in-service testing program.

SURVEILLANCE REQUIREMENTS (continued)

SR 3.6.6.3 and SR 3.6.6.4

These SRs demonstrate each automatic containment spray valve actuates to its correct position and that each containment spray pump starts upon receipt of an actual or simulated containment spray actuation signal. 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.

SR 3.6.6.5

With the containment spray inlet valves closed and the containment spray header drained, 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 nature of the design of the nozzle, a test at the first fuel loading and at 10-year intervals is considered adequate to detect obstruction of the spray nozzles.

SR 3.6.6.6

Verifying that the containment spray header piping is full of water to the 26.213 m (86 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.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 38, 39, 40, 41, 42, and 43.
2. DCD Tier 2, Subsection 6.2.2.
3. 10 CFR 50.34.
4. ASME OM Code.
5. APR1400-Z-A- NR-13007-P, “Technical Report of LOCA M/E Methodology,” July 2013.

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.

Five MSSVs are located on each main steam header (ten MSSVs per one steam generator), outside containment, upstream of the main steam isolation valves, as described in the DCD Tier 2, Section 5.2 and 5.4 (Reference 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 (Reference 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 less than or equal 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 DCD Tier 2, Section 15.2 (Reference 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 peak pressure is less than 110 % of the design pressure of 2500 psia, but high enough to actuate the pressurizer safety valves.

APPLICABLE SAFETY ANALYSES (continued)

The maximum relieving rate during the LOCV event is less than the rated capacity of two MSSVs.

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 peak pressure is less than 110 % of the design pressure of 2500 psia with the pressurizer safety valves providing relief capacity. The maximum relieving rate of the MSSVs during the FWLB event 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 exceeding 110 % (2750 psia) of design pressure. This is considered acceptable as RCS pressure is still well below 120 % of design pressure where deformation could occur. The probability of this event is in the range of 4×10^{-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 fully 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.

LCO (continued)

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.

APPLICABILITY

In MODE 1, a minimum of five 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 MSSVs per Table 3.7.1-1 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 %.

$$\text{Allowable THERMAL POWER} = \left(\frac{10 - N}{10} \right) \times 107.55$$

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.

ACTIONS (continued)

SP = Allowable THERMAL POWER + 9.4

where:

SP = Reduced reactor trip setpoint in % RTP. This is a ratio of the available relieving capacity over the total steam flow at rated power.

10 = Total number of MSSVs per steam generator.

N = Number of inoperable MSSVs on the steam generator with the greatest number of inoperable valves.

107.55 = 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).

9.4 = 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.

ACTIONS (continued)

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 four 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 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 3.7.1.1

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 (Reference 4), requires that safety and relief valve tests be performed in accordance with ANSI/ASME OM-1-1987 (Reference 5). According to Reference 5, the following tests are required for MSSVs:

a. Visual examination

b. Seat tightness determination

c. Setpoint pressure determination (lift setting)

d. Compliance with owner's seat tightness criteria

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.

SURVEILLANCE REQUIREMENTS (continued)

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. DCD Tier 2, Section 5.2 and 5.4.
2. ASME Section III, Article NC-7000, Class 2 Components.
3. DCD Tier 2, Section 15.2.
4. ASME OM Code.
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, Turbine Bypass System, and other auxiliary steam supplies from the steam generators.

The MSIVs close on a main steam isolation signal generated by high steam generator level, low steam generator pressure, and 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 DCD Tier 2, Section 10.3 (Reference 1).

APPLICABLE SAFETY ANALYSIS

The design basis of the MSIVs is established by the containment for the large steam line break (SLB) inside containment, as discussed in the DCD Tier 2, Section 6.2 (Reference 2). It is also influenced by the accident analysis of the SLB events presented in the DCD Tier 2, Section 15.1.5 (Reference 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.

APPLICABLE SAFETY ANALYSES (continued)

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 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. 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.

APPLICABLE SAFETY ANALYSES (continued)

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.

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. Steam generator tube rupture

For this scenario, closure of the MSIVs 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.

The MSIVs are also used 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 four 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 (Reference 4) limits or the NRC staff approved licensing basis.

BASES

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.

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 4-hour Completion Time is reasonable, considering the probability of an accident occurring during the time period that would require closure of the MSIVs.

The 4-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 and C.2

Condition C is modified by a Note indicating that separate Condition entry is allowed for each MSIV.

BASES

ACTIONS (continued)

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 4-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 MCR, and other administrative controls, to ensure these valves are in the closed position.

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 within the limit given in Reference 5 and is within that assumed in the accident and containment analyses. This SR also verifies the valve closure time is in accordance with the Inservice Testing Program. 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 (Reference 6) requirements during operation in MODES 1 and 2.

The Frequency for this SR is in accordance with the Inservice Testing Program.

SURVEILLANCE REQUIREMENTS (continued)

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.

REFERENCES

1. DCD Tier 2, Section 10.3.
2. DCD Tier 2, Section 6.2.
3. DCD Tier 2, Subsection 15.1.5.
4. 10 CFR 100.11.
5. Technical Requirement Manual
6. ASME OM Code.

B 3.7 PLANT SYSTEMS

B 3.7.3 Main Feedwater Isolation Valves (MFIVs)

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 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 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 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 (AF) to the intact loop.

Two MFIVs are located on each AF line, outside, but close to, containment. The MFIVs are located upstream of the AF injection point so that AF can 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 AF reaching the steam generator following either an SLB or FWLB.

The MFIVs close on receipt of a main steam isolation signal (MSIS) generated by any one of low steam generator pressure, high steam generator level, and high containment pressure. The MSIS also actuates the main steam isolation valves (MSIVs) to close. The MFIVs can also be actuated manually. In addition to the MFIVs, 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 DCD Tier 2, Subsection 10.4.7 (Reference 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 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 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 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 in each feedwater line be OPERABLE. The MFIVs 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 could result in the introduction of water into the main steam lines.

APPLICABILITY

The MFIVs 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 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, they are already performing their safety function.

APPLICABILITY(continued)

In MODES 4, 5, and 6, steam generator energy is low. Therefore, the MFIVs are normally closed since MFW is not required.

ACTIONS

The ACTIONS Table is modified by a Note indicating that separate Condition entry is allowed for each valve.

A.1 and A.2

With one MFIV inoperable, action must be taken to close or isolate the inoperable valves within 72 hours. When these valves are closed or isolated, they are performing their required safety function (i.e., to isolate the line).

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 and B.2

If more than one MFIV 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 otherwise isolate the affected flow path.

Inoperable MFIVs 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 MCR, and other administrative controls to ensure that these valves are closed or isolated.

ACTIONS (continued)

C.1 and C.2

If the MFIVs 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 verifies that the closure time of each MFIV is within the limit given in Reference 2 and is within that assumed in the accident and containment analyses. This SR also verifies that the valve closure time is in accordance with the Inservice Testing Program. This SR 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 (Reference 3) 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 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. DCD Tier 2, Subsection 10.4.7.
2. Technical Requirements Manual.
3. ASME OM Code.

B 3.7 PLANT SYSTEMS

B 3.7.4 Main Steam Atmospheric Dump Valves (MSADVs)

BASES

BACKGROUND

The MSADVs provide a safety grade method for cooling the unit to shutdown cooling system (SCS) entry conditions, should the preferred heat sink via the Steam Bypass System to the condenser not be available, as discussed in the DCD Tier 2, Section 10.3 (Reference 1). This is done in conjunction with the auxiliary feedwater system providing cooling water from the auxiliary feedwater storage tank (AFWST). The MSADVs could 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 MSADV lines are provided. Each MSADV line consists of one MSADV and an associated block valve. Two MSADV 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 MSADVs are provided with upstream block valves to permit their being tested at power, and to provide an alternate means of isolation. The MSADVs are electro-hydraulically operated and include internal solenoid operated pilot valves and electronic valve positioners to permit control of the cooldown rate.

A description of the MSADVs is found in Reference 1. The MSADVs are OPERABLE with only a DC power source available. In addition, hand wheels or manual control provisions are provided to enable manual operation of the electro-hydraulic operator mounted on the valve upon total loss of power.

APPLICABLE SAFETY ANALYSES

The design basis of the MSADVs is established by the capability to cool the unit to SCS System entry conditions. A cooldown rate of 41.7 °C (75 °F) per hour is obtainable by one or both steam generators. This design is adequate to cool the unit to SCS System entry conditions with only one MSADV and one steam generator, using the cooling water supply available in the AFWST.

APPLICABLE SAFETY ANALYSES (continued)

In the accident analysis presented in the DCD Tier 2, the MSADVs are assumed to be used by the operator to cool down the unit to SCS 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 could 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 MSADV 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 MSADVs on the affected steam generator could still be available following a SGTR event).

The design must accommodate the single failure of one MSADV to open on demand; thus, each steam generator must have at least two MSADVs. The MSADVs are equipped with block valves in the event an MSADV spuriously opens, or fails to close during use.

The MSADVs satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

Two MSADV lines are required to be OPERABLE on each steam generator to ensure that at least one MSADV 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 MSADV line on the unaffected steam generator. The block valves must be OPERABLE to isolate a failed open MSADV. A closed block valve does not render it or its MSADV 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 SCS System entry conditions following an event in which the condenser is unavailable for use with the steam bypass system.

An MSADV 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 MSADVs are required to be OPERABLE.

In MODES 5 and 6, an SGTR is not a credible event.

ACTIONS

A.1

With one required MSADV 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 MSADV lines, and a nonsafety grade backup in the Steam Bypass System and MSSVs.

B.1

With two MSADV lines inoperable, action must be taken to restore one of the MSADV lines to OPERABLE status. As the block valve can be closed to isolate an MSADV, some repairs could be possible with the unit at power. The 24-hour Completion Time is reasonable to repair inoperable MSADV 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 MSADV lines.

C.1 and C.2

If the MSADV 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.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.7.4.1

To perform a controlled cooldown of the RCS, the MSADVs must be able to be opened and throttled through their full range. This SR ensures the MSADVs are tested through a full control cycle at least once per fuel cycle. Performance of inservice testing or use of an MSADV during a unit cooldown can 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.

SR 3.7.4.2

The function of the MSADV block valve is to isolate a failed open MSADV. 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 can 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. DCD Tier 2, Section 10.3.

B 3.7 PLANT SYSTEMS

B 3.7.5 Auxiliary Feedwater System (AFWS)

BASES

BACKGROUND

The AFWS automatically supplies feedwater to the steam generators to remove decay heat from the reactor coolant system upon the loss of normal feedwater supply. The auxiliary feedwater (AFW) pumps take suction through separate and independent suction lines from the auxiliary feedwater storage tanks (AFWSTs) (LCO 3.7.6) and pump to the steam generator secondary side via a separate and independent connection to the main feedwater (MFW) piping inside containment. The steam generator functions 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) or main steam atmospheric dump valves (MSADVs) (LCO 3.7.4). If the main condenser is available, steam may be released to the main condenser via the turbine bypass valves.

The AFWS consists of two motor driven AFW pumps and two steam turbine driven pumps configured into four trains. Each motor driven pump provides 100 % of AFW flow capacity and each turbine driven pump provides 100 % of the required capacity to its respective steam generator as assumed in the accident analysis. The pumps are equipped with independent recirculation lines to prevent pump operation against close system.

Each motor driven AFW pump is powered from an independent Class 1E power supply, and feeds one steam generator. One pump at full flow is sufficient to remove decay heat and cool the unit to shutdown cooling system (SCS) entry conditions.

Each turbine driven AFW pump receives steam from an independent main steam line, 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 feedwater to the steam generator which provides driving steam, with DC-powered control valves actuated by the auxiliary feedwater actuation signal (AFAS).

BACKGROUND (continued)

The AFW system supplies feedwater to the steam generators upon the loss of normal feedwater supply.

The AFW System is designed to supply sufficient water to the steam generators 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 shutdown cooling system entry conditions, and steam is released through the MSADVs.

The AFWS actuates automatically on low steam generator level by the AFAS as described in LCO 3.3.5, “Engineered Safety Feature Actuation System (ESFAS) Instrumentation.” The AFAS logic is designed to feed its respective steam generators with low levels, but the AFW flow to the ruptured steam generator is terminated manually by operator action within 30 minutes after the secondary side pipe rupture event. The AFAS automatically actuates the AFW turbine driven pump and associated DC-operated valves and control 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 AFWS is discussed in Subsection 10.4.9 (Reference 1).

APPLICABLE SAFETY ANALYSES

The AF system mitigates the consequences of any event with a loss of normal feedwater. The design basis of the AFWS 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 against a steam generator feedwater nozzle pressure of 87.2 kg/cm^{2}A (1,240 psia).

The limiting design basis accidents (DBAs) and transients for the AFWS are as follows:

a. Feedwater line break (FWLB)

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.

APPLICABLE SAFETY ANALYSES (continued)

The AFWS design is such that it can perform its function following an FWLB between the main feed water isolation valve and containment, combined with a loss of offsite power following turbine trip, and a single active failure of the turbine driven AFW pump. The AFW flow to the faulted steam generator is terminated manually by the operator action. Sufficient flow would be delivered to the intact steam generator by the redundant AFW pump.

The AFWS satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

The LCO requires that four independent AFW trains be OPERABLE to ensure that the AFWS will perform the design safety function to mitigate the consequences of accidents that could result in overpressurization of the reactor coolant pressure boundary. Four independent AFW pumps, in four diverse trains, ensure availability of residual heat removal capability for all events accomplished by a loss of offsite power and a single failure. This is accomplished by powering two pumps from independent emergency buses. The third and fourth AFW pumps are powered by a diverse means, two steam driven turbines supplied with steam from an independent source not isolated by the closure of the MSIVs.

The AFWS 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 flow to a separate steam generator. Two turbine driven AFW pumps shall be OPERABLE with steam supplies from the main steam lines upstream of the MSIVs, and each capable of supplying AFW flow to the steam generators which provides driving steam. The piping, valves, instrumentation, and controls in the required flow paths shall also be OPERABLE.

The LCO is modified by a Note indicating that one AFW train, which includes a motor driven pump, is required to be OPERABLE in MODE 4 when a steam generator is relied upon for heat removal. 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 AFWS is required to be OPERABLE and to function in the event that the main feed water is lost. In addition, the AFWS 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 AFWS may be used for heat removal via a steam generator.

In MODES 5 and 6, the steam generators are not normally used for decay heat removal, and the AFWS is not required.

ACTIONS

A.1

If one turbine driven AFW pump is inoperable due to inoperable steam supply, or if a turbine driven pump is inoperable for any reason 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 one turbine driven AFW pump due to associated inoperable steam supply, the 7-day Completion Time is reasonable due to the redundancy afforded by the remaining OPERABLE turbine driven train.

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 one turbine driven pump due to inoperable steam supply 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 pumps.

Condition A is modified by a Note which limits the applicability of the Condition for an inoperable turbine driven AFW pump in MODE 3 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.

ACTIONS (continued)

This longer Completion Time is based on the reduced decay heat following refueling and prior to the reactor being critical.

B.1

With one of the required AFW trains (pump or flow path) inoperable in MODE 1, 2, or 3 for reasons other than Condition A, action must be taken to restore OPERABLE status within 72 hours. The 72-hour Completion Time is reasonable based on the redundant capabilities afforded by the AFWS, the time needed for repairs, and the low probability of a DBA event occurring during this period. Three AFW pumps and flow paths remain to supply feedwater to the steam generators.

C.1 and C.2

With one of the required motor driven AFW trains (pump or flow path) inoperable and one required turbine driven AFW train inoperable due to associated inoperable steam supply, action must be taken to restore the affected equipment to OPERABLE status within 48 hours. Assuming no single active failures when in this condition, the accident (a FLB or MSLB) could result in the loss of the steam supply to the remaining turbine driven AFW pump due to the faulted steam generator (SG). In this condition, the AFWS may no longer be able to meet the required flow to the SGs assumed in the safety analysis, either due to the analysis requiring flow from two AFW pumps or due to the remaining AFW pump having to feed a faulted SG.

The 48-hour Completion Time is reasonable based on the fact that the remaining motor driven AFW train is capable of providing 100 % of the AFW flow requirements and the low probability of an event occurring that would challenge the AFWS.

D.1 and D.2

When Required Action A.1, B.1, C.1, or C.2 cannot be completed within the required 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 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.

ACTIONS (continued)

In MODE 4, with three AFW trains inoperable in MODE 1, 2, or 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 Shutdown Cooling.

E.1

Required Action E.1 is modified by a Note indicating that all required MODE changes are suspended until one AFW train is restored to OPERABLE status.

With all four AFW trains inoperable in MODES 1, 2, or 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 non-safety grade equipment. In such a condition, the unit should not be perturbed by any action, including a power change, that may 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.

F.1

Required Action F.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 SC 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 flow paths provides assurance that the proper flow paths exist for AFW operation. This SR does not apply to valves which 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.

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 OM Code (Reference 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 in-service tests confirm component OPERABILITY, trend performance, and detect incipient failures by indicating abnormal performance. Performance of in-service testing, discussed in the ASME OM Code (Reference 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 AFAS 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.

SURVEILLANCE REQUIREMENTS (continued)

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.

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 AFAS 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.

SR 3.7.5.5

This SR ensures that the AFWS 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, 6, or defueled. OPERABILITY of AFW flow paths must be verified before sufficient core heat is generated that would require the operation of the AFWS during a subsequent shutdown.

SURVEILLANCE REQUIREMENTS (continued)

The Frequency is reasonable, based on engineering judgment, and other administrative controls to ensure that flow paths remain OPERABLE. To further ensure AFWS alignment, the OPERABILITY of the flow paths is verified following extended outages to determine that no misalignment of valves has occurred. This SR ensures that the flow path from the AFWST to the steam generators is properly aligned by requiring a verification of minimum flow capacity of 650 gpm at 1,240 psia. (This SR is not required by those units that use AFW for normal startup and shutdown.)

REFERENCES

1. DCD Tier 2, Subsection 10.4.9.

2. ASME OM Code.

B 3.7 PLANT SYSTEMS

B 3.7.6 Auxiliary Feedwater Storage Tank (AFWST)

BASES

BACKGROUND

The AFWST provides a safety grade source of water to the steam generators for removing decay and sensible heat from the reactor coolant system (RCS). The AFWST provides a passive flow of water, by gravity, to the auxiliary feedwater (AFW) pumps (LCO 3.7.5). The steam produced is released to the atmosphere by the main steam safety valves (MSSVs) or the main steam atmospheric dump valves (MSADVs). The AFW pumps operate with a continuous recirculation to the AFWST.

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 turbine bypass valves. This has the advantage of conserving condensate while minimizing releases to the environment.

Because the AFWST is a principal component in removing residual heat from the RCS, it is designed to withstand earthquakes and other natural phenomena. The AFWST is designed to seismic Category I requirements to ensure availability of the feedwater supply. Feedwater is also available from one of two 100 % capacity AFWSTs as backup water sources.

A description of the AFWST is provided in Subsection 10.4.9 (Reference 1).

APPLICABLE SAFETY ANALYSES

The AFWST provides cooling water to remove decay heat and cooldown the unit following all events in the accident analysis, Chapter 6 and 15. For anticipated operating 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 (SC) entry conditions at the design cooldown rate.

APPLICABLE SAFETY ANALYSES (continued)

The limiting event for the AFW 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 emergency diesel generator powering the motor driven AFW pump to the unaffected steam generator (requiring additional steam to drive the remaining AFW pump turbine)

b. The failure of the turbine 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 AFWST 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 Auxiliary 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 AFWST satisfies Criteria 2 and 3 of 10 CFR 50.36(c)(2)(ii).

LCO

To satisfy accident analysis assumptions, the AFWST must contain sufficient cooling water to remove decay heat for 30 minutes following a reactor trip from 102 % RTP and then cooldown the RCS to SC entry conditions, assuming a loss of offsite power and the most adverse single failure. In doing this it must retain sufficient water to ensure adequate NPSH 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 AFWST level required is a usable volume of greater than or equal to 1,524,165 L (400,000 gal), which is based on holding the unit in MODE 3 for 8 hours followed by a cooldown to SC entry conditions at 41.7 °C (75 °F) per hour. This bases is established by the BTP RSB 5-4 (Reference 4) and exceeds the volume required by the accident analysis.

OPERABILITY of the AFWST is determined by maintaining the tank level at or above the minimum required level.

BASES

APPLICABILITY

In MODE 1, 2, and 3, and in MODE 4, when a steam generator is relied upon for heat removal, the AFWST is required to be OPERABLE.

In MODES 5 and 6, the AFWST is not required because the AFW System is not required.

ACTIONS

A.1 and A.2

If one AFWST is not OPERABLE, the OPERABILITY of the other AFWST must be verified by administrative means within 4 hours and once every 12 hours thereafter.

OPERABILITY of the other AFWST must include verification of the OPERABILITY of flow paths from the tank to the AFW pumps, and availability of the required volume of water. The AFWST must be returned to OPERABLE status within 7 days. The 4-hour Completion Time is reasonable, based on operating experience, to verify the OPERABILITY of the other AFWST. Additionally, verifying the OPERABILITY of the other AFWST every 12 hours is adequate to ensure the AFW supply continues to be available. The 7-day Completion Time is reasonable, based on an OPERABLE AFWST being available and the low probability of an event requiring the use of the water from the AFWST occurring during this period.

B.1 and B.2

If the AFWST 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 generators 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 each AFWST contains the required volume of cooling water. (This level greater than or equal to 1,524,165 L (400,000 gal)) The 12-hour Frequency is based on operating experience and the need for operator awareness of unit evolutions that could affect the AFWST inventory between checks. The 12-hour Frequency is considered adequate in view of other indications in the MCR, including alarms, to alert the operator to abnormal AFWST level deviations.

REFERENCES

1. DCD Tier 2, Subsection 10.4.9.
2. DCD Tier 2, Chapter 6.
3. DCD Tier 2, Chapter 15.
4. NUREG-0800, BTP 5-4, Rev. 3, March 2007.

B 3.7 PLANT SYSTEMS

B 3.7.7 Component Cooling Water System (CCWS)

BASES

BACKGROUND

The component cooling water system (CCWS) is a closed loop cooling water system which cools components and heat exchangers connected to the CCWS. The CCWS is capable of removing sufficient heat using various combinations of pumps and heat exchangers to:

a. Ensure a safe reactor shutdown coincident with loss of offsite power.

b. Perform a normal shutdown cooling of the reactor within 24 hours.

c. Perform a safe shutdown cooling of the reactor within 24 hours.

d. Perform post-LOCA cooling.

e. Perform normal power operation cooling.

The CCWS consists of two separate, independent, redundant, closed loop, safety related divisions. Either division of the CCWS is capable of supporting 100 % of the cooling functions required for a safe reactor shutdown.

Each division of the CCWS includes three CCW heat exchangers, a surge tank, two CCW pumps, a chemical addition tank, a component cooling water radiation monitor, piping, valves, controls, and instrumentation. The CCWS provides cooling water to essential and non-essential components.

The non-essential headers are isolated automatically on an SIAS. If these headers fail to isolate, the idle CCW pump in the respective loop will automatically start on a low pump discharge common header pressure signal. This assures that there is no flow degradation to the safety related components. The non-essential headers and the RCP headers lines isolate on a low-low surge tank level.

BACKGROUND (continued)

Makeup water to the CCWS is normally supplied by the makeup demineralized system. The backup makeup water source is from the auxiliary feedwater (AFW) system.

The CCWS serves as an intermediate cooling water system between the radioactive systems and the ESWS. A radiation monitor is provided at the outlet of the component cooling water pumps to detect any radioactive leakage into the CCWS.

Additional information on the design and operation of the system, along with a list of components served, can be found in Chapter 9 (Reference 1).

APPLICABLE SAFETY ANALYSES

The CCWS, in conjunction with the essential service water system (ESWS) and the ultimate heat sink (UHS), is capable of removing sufficient heat from the essential heat exchangers to ensure a safe reactor shutdown and cooling following a postulated accident coincident with a loss of offsite power.

The CCWS, in conjunction with the ESWS, is capable of maintaining the outlet temperature of the CCW heat exchanger within the limits of 18.33 °C (65 °F) and 43.33 °C (110 °F) during a design basis accident with loss of offsite power. This can be attained with one CCW pump and one ESW pump in a single division.

For a safe shutdown, the CCWS, in conjunction with the SCS and ESWS, are designed to cool the reactor coolant from 176.7 °C (350 °F) to 93.3 °C (200 °F) through the shutdown cooling heat exchangers and the component cooling water heat exchangers. The reactor can be cooled to 93.3 °C (200 °F) within 24 hours after reactor shutdown by first cooling the reactor coolant to 176.7 °C (350 °F) through a steam generator and then cooling to 93.3 °C (200 °F) using one SCS pump, one ESW pump and one CCW pump in a single division of the SCS, CCWS, and ESWS. The CCW flow to non-safety heat loads has to be isolated.

A single failure of any component in the CCWS will not impair the ability of the CCWS to meet its safety functional requirements.

APPLICABLE SAFETY ANALYSES (continued)

For the normal shutdown, the CCWS, in conjunction with the SCS and ESWS, is designed to cool the reactor coolant from 176.7 °C (350 °F) to 60.0 °C (140 °F) through the shutdown cooling heat exchangers and the CCW heat exchangers. The reactor can be cooled to 60.0 °C (140 °F) within 24 hours after reactor shutdown by first cooling the reactor coolant to 176.7 °C (350 °F) through the steam generators and then cooling to 60.0 °C (140 °F) by using both divisions of SCS, CCWS, and ESWS.

The CCWS satisfies LCO SELECTION CRITERION 3.

LCO

The CCWS divisions are independent of each other to the degree that each has separate controls, power supplies, and the operation of one does not depend on the other. In the event of a DBA, one CCWS division 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 divisions of CCWS must be OPERABLE. At least one division will operate assuming the LCO worst single active failure occurs coincident with the loss of offsite power.

A division is considered OPERABLE when:

a. Pump and associated surge tank are OPERABLE.

b. Associated piping, valves, two heat exchangers, and instrumentation and controls required to perform safety related functions are OPERABLE.

The isolation of CCW to non-safety-related components or systems can render those components or systems inoperable, but does not affect the OPERABILITY of the CCWS.

APPLICABILITY

In MODES 1, 2, 3, and 4 the CCWS is a normally operating system, which must be available to perform its post-accident safety functions, primarily RCS heat removal, by cooling the shutdown cooling heat exchanger.

In MODES 5 and 6, the OPERABILITY requirements of the CCWS are determined by the systems it supports.

BASES

ACTIONS

A.1

Required Action A.1 is modified by two Notes. The first indicates the requirement of entry into the applicable Conditions and Required Actions of LCO 3.8.1, “AC Sources – Operating,” for emergency diesel generator inoperable by CCW. The second indicates the requirement of entry into the applicable Conditions and Required Actions of LCO 3.4.6, “RCS Loops – MODE 4,” for SCS inoperable by CCW. These are exceptions to LCO 3.0.6 and ensure the proper ACTIONS are taken for these components.

In MODE 1, 2, 3, or 4 with one CCW division inoperable, action must be taken to restore OPERABLE status within 72 hours. In this Condition, the remaining OPERABLE CCW division is capable to perform the heat removal function. The 72-hour Completion Time is based on the redundant capabilities afforded by the OPERABLE division and the low probability of a DBA occurring during this period.

B.1 and B.2

If the CCW division 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 is available for CCW operation. This SR does not apply to valves which are locked, sealed, or otherwise secured in position, since they were verified to be in the correct position prior to locking, sealing, or securing. This SR also does not apply to valves which 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 positions.

SURVEILLANCE REQUIREMENTS (continued)

This SR is modified by a Note indicating that the isolation of the CCW components or systems can render those components inoperable but does not affect the OPERABILITY of the CCWS.

The 31-day Frequency, based on engineering judgment, is consistent with the procedural controls governing valve operation and ensures correct valve positions.

SR 3.7.7.2

This SR verifies proper automatic operation of the CCW valves on an actual or simulated actuation signal. The CCWS 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 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 CCWS 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. DCD Tier 2, Subsection 9.2.2.

B 3.7 PLANT SYSTEMS

B 3.7.8 Essential Service Water System (ESWS)

BASES

BACKGROUND

The essential service water system (ESWS) provides a heat sink for the removal of process and operating heat from safety related components during a transient or DBA. During normal operation or a normal shutdown, the ESWS also provides this function for various safety-related and non-safety-related components through the component cooling water system (CCWS).

The ESWS consists of two separate, redundant, open loop, safety-related divisions. Each division cools one of two divisions of the CCWS, which in turn cools 100 % of the safety-related loads. The ESWS operates at a lower pressure than the CCWS to prevent contamination of the CCWS with raw water.

Each division of the ESWS consists of two pumps, three debris filters and associated piping, valves, controls and instrumentation. The ESW pumps circulate cooling water to the CCW heat exchanger and back to the ultimate heat sink. Provisions are made to ensure a continuous flow of cooling water under normal and accident conditions.

Additional information on the design and operation of the system, along with a list of the components served, can be found in Chapter 9.2.1 (Reference. 1).

APPLICABLE SAFETY ANALYSES

The ESWS, in conjunction with the CCWS and ultimate heat sink (UHS), is capable of removing sufficient heat to ensure a safe reactor shutdown coincident with a loss of offsite power.

The ESWS is capable of maintaining the CCWS supply temperature of 43.33 °C (110°F) or less following the DBA under the most adverse historical meteorological conditions consistent with the intent of NRC RG 1.27. This can be attained with one ESW pump in a single division.

APPLICABLE SAFETY ANALYSES (continued)

For a safe shutdown, the ESWS, in conjunction with the SCS and CCWS, are designed to cool the reactor coolant from 176.7 °C (350°F) to 93.3 °C (200°F) through the SC heat exchangers and the CCW heat exchangers. The reactor can be cooled to 93.3 °C (200°F) within 24 hours after reactor shutdown by first cooling the reactor coolant to 176.7 °C (350°F) through a steam generator and then cooling to 93.3 °C (200°F) using one SCS pump, one ESW pump, and one CCW pump in a single division of the SCS, CCWS, and ESWS. The CCW flow to non-safety heat loads has to be isolated.

A single failure of any component in the ESWS will not impair the ability of the ESWS to meet its functional requirements.

For the normal shutdown, the ESWS, in conjunction with the CCWS and SCS, is designed to cool the reactor coolant from 176.7 °C (350°F) to 60 °C (140°F) through the SC heat exchangers and the CCW heat exchangers. The reactor coolant can be cooled to 60 °C (140°F) within 24 hours after reactor shutdown by first cooling the reactor coolant to 176.7 °C (350°F) through the steam generators and then cooling the reactor coolant to 60 °C (140°F) by using both divisions of the SCS, CCWS, and ESWS.

The ESWS, in conjunction with the CCWS, is designed to provide a maximum CCW temperature of 35.0 °C (95°F) or less during normal operating MODES.

The ESWS satisfies LCO SELECTION CRITERION 3.

LCO

Two ESWS divisions provide the required redundancy to ensure the system functions to remove post-accident heat loads, assuming the worst single active failure occurs coincident with the loss of offsite power.

An ESWS division is considered OPERABLE when:

a. An associated pump is OPERABLE.

b. The associated piping, valves, and instrumentation and controls required to perform the safety related functions are OPERABLE.

BASES

APPLICABILITY

In MODES 1, 2, 3, and 4 the ESWS system is a normally operating system, which is required to support the OPERABILITY of the equipment serviced by the ESWS and required to be OPERABLE in these MODES.

In MODES 5 and 6, the OPERABILITY requirements of the ESWS are determined by the systems it supports.

ACTIONS

A.1

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 ESWS division 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 ESWS division results in an inoperable shutdown cooling. These are exceptions to LCO 3.0.6 and ensure the proper ACTIONS are taken for these components.

In MODES 1, 2, 3, and 4 with one ESWS division inoperable, action must be taken to restore OPERABLE status within 72 hours. In this Condition, the remaining OPERABLE ESWS division is adequate to perform the heat removal function. However, the overall reliability is reduced because a single failure in the ESWS divisions could result in loss of ESWS function.

The 72-hour Completion Time is based on the redundant capabilities afforded by the OPERABLE division and the low probability of a DBA occurring during this time period.

B.1 and B.2

The unit must be placed in a MODE in which the LCO does not apply if the ESWS division cannot be restored to OPERABLE status in the associated Completion Time. This is done by placing the plant in at least MODE 3 in 6 hours and MODE 5 in 36 hours. The allowed Completion Times are reasonable based on operating experience to reach the required MODES from full power operation without challenging unit systems.

SURVEILLANCE REQUIREMENTS

SR 3.7.8.1

Verifying the correct alignment for manual, power operated, and automatic valves in the ESWS flow path ensures that the proper flow paths exist for ESWS 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 ESWS components or systems can render those components inoperable but does not affect the OPERABILITY of the ESWS.

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 ESWS valves on an actual or simulated actuation signal. The ESWS 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.

SURVEILLANCE REQUIREMENTS (continued)

SR 3.7.8.3

The SR verifies proper automatic operation of the ESWS pumps on an actual or simulated actuation signal. The ESWS 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. DCD Tier 2, Subsection 9.2.1.

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 by using the essential service water system (ESWS) and the component cooling water system (CCWS).

The safety function of the UHS is to dissipate the maximum heat load of all modes of operation including that of a LOCA and LOOP under the worst combination of adverse environmental conditions.

[[The UHS consists of two independent, redundant, safety related divisions. Each division cools one of two divisions of the ESWS, which in turn cools 100 % of the safety-related loads. Each division of UHS consists of two mechanical draft cooling towers, associated basin, piping, valves, controls and instrumentation. Each cooling tower consists of three 33 1/3 % capacity cells with fans and motors. Each cooling tower rejects heat from the Essential Service Water (ESW) to ambient and returns the cooled water to the UHS cooling tower basin, from which the ESW pumps take suction. Each UHS cooling tower basin is sized for 3 days of safe shutdown or post-accident operation and ensures adequate volume for the required net positive suction head (NPSH) for the associated ESW pump. Post-accident evaporation and other losses are replenished by a seismic Category I makeup water source. The seismic Category I makeup water source delivers water to each basin at greater than or equal to 2,362 L/min (624 gpm) to maintain the NPSH for the ESW pump for up to 30 days of safe shutdown or post-accident.]]

[[The four mechanical draft cooling towers and two basins are safety related, seismic Category I structures sized to provide heat dissipation for safe shutdown or post-accident. The cooling tower is protected from tornadoes, external missiles, and seismic phenomena.]]

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.

[[The seismic Category I makeup necessary to support 30 days of post-accident mitigation is site specific and details are to be provided by the combined license (COL) applicant.]]

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 ANALYSIS

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.

The operating limits are based on 3.5 hours after shutdown. [[A conservative heat transfer analysis for the worst case accident was performed to ensure that the cooling tower capacity and the basin water inventory adequately remove the heat load for the worst case accident.]] The UHS is designed in accordance with NRC RG 1.27 (Reference. 2), which requires a 30-day supply of cooling water in the UHS.

The UHS satisfies LCO SELECTION CRITERION 3.

LCO

[[One UHS system division is required to ensure that the system functions to remove post-accident or safe shutdown heat loads. To ensure that this requirement is met, two divisions of UHS system must be OPERABLE, assuming the worst single active failure occurs coincident with the loss of offsite power.]]

[[A]] UHS [[division]] is considered OPERABLE when:

a. [[Cooling tower fans in a cooling tower are OPERABLE.]]

b. [[The associated piping, valves, and instrumentation and controls required to perform the safety-related function are OPERABLE.]]

c. Water temperature of the UHS is less than or equal to [[33.2 °C (91.8 °F)]] and water level of the UHS is greater than or equal to [[10 feet from the bottom of basin with capability to makeup from OPERABLE makeup source during normal operation.]] Definition of OPERABLE makeup source is to be provided by the COL applicant.

BASES

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.

ACTIONS

A.1

[[If one UHS division is inoperable, action must be taken to restore the inoperable cooling tower(s) and associated fan(s) to OPERABLE status within 72 hours. In this Condition, the remaining OPERABLE UHS division is adequate to perform the heat removal function. However, the overall reliability is reduced because a single failure in the UHS division could result in loss of UHS function.

The 72-hour Completion Time is based on the redundant capabilities afforded by the OPERABLE division and the low probability of a DBA occurring during this time period.]]

B.1

If [[the Required Actions and Completion Times of Condition A are not met, or]] the UHS is inoperable [[for reasons other than Condition A]], 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 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 short term (3 days) cooling can be maintained. The level specified also ensures sufficient NPSH is available for operating the ESW pumps [[during the first 3 days]] following DBA or safe shutdown with LOOP. 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 greater than or equal to [[3 m (10 ft) from the bottom of the basin.]]

SR 3.7.9.2

This SR verifies that the ESWS is available to cool the CCWS 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 less than or equal to [[33.2 °C (91.8 °F).]]

SR 3.7.9.3

[[Operating each cooling tower fans for greater than or equal to 15 minutes verify 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.]]

SR 3.7.9.4

[[This SR verifies the correct alignment for manual, power operated, and automatic valves in the UHS flow path ensures that the proper flow paths exist for UHS 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.]]

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 3.7.9.5

[[This SR verifies proper automatic operation of the UHS valves on an actual or simulated actuation signal. The UHS 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.]]

SR 3.7.9.6

[[The SR verifies proper automatic operation of the cooling tower fans on an actual or simulated actuation signal. The UHS 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.]]

SR 3.7.9.7

[[This SR verifies that adequate long term (30 days) cooling can be maintained. The specific seismic Category I UHS makeup pump flowrate ensures that sufficient NPSH can be maintained to operate the ESW pumps following the first 3 days post-LOCA. The Frequency is in accordance with the In-service Testing Program and is in accordance with the ASME OM Code (Reference. 3). This SR verifies that the UHS makeup pump flowrate is greater than or equal to 2,362 L/min (624 gpm).]]

REFERENCES

1. DCD Tier 2, Subsection 9.2.5.

2. NRC RG 1.27, Rev. 2, January 1976.

[[3. ASME OM Code.]]

B 3.7 PLANT SYSTEMS

B 3.7.10 Essential Chilled Water System (ECWS)

BASES

BACKGROUND

The ECWS 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 ECWS is a closed loop system consisting of two independent divisions. Each 100 % capacity division includes two 100 % capacity chillers and chilled water pumps, a compression tank, a chilled water makeup pump, an air separator, a chemical addition tank, piping, valves, controls, and instrumentation. An independent, 100 % capacity chilled water refrigeration unit cools each division. The ECWS supplies chilled water to the heating, ventilation, and air conditioning (HVAC) units in engineered safety feature (ESF) equipment areas (e.g., main control room, electrical equipment room, safety injection pump area).

Additional information about the design and operation of the system, along with a list of components served, can be found in Subsection 9.2.7 (Reference 1).

APPLICABLE SAFETY ANALYSES

The design basis of the ECWS is to remove the post-accident heat load from ESF spaces following a DBA coincident with a loss of offsite power. Each division provides chilled water to the HVAC units at the design temperature of 5.6 °C (42 °F).

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 IRWST is supplied to the safety injection (SI) and containment spray pumps. This heat load to the area atmosphere must be removed by the ECWS to ensure these systems remain OPERABLE.

The ECWS satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO

Two ECWS divisions 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 ECWS division is considered OPERABLE when:

a. One chiller, chilled water pump, chilled water makeup pump and compression tank are OPERABLE.

b. The associated piping, valves, refrigeration unit, and instrumentation and controls required to perform the safety-related function are OPERABLE.

APPLICABILITY

In MODES 1, 2, 3, and 4 the ECWS is required to be OPERABLE when a LOCA or other accidents would require ESF operation.

In MODES 5 and 6, potential heat loads are smaller and the probability of accidents requiring the ECWS is low.

ACTIONS

A.1

If one ECWS division is inoperable, action must be taken to restore OPERABLE status within 7 days. In this condition, one OPERABLE ECWS division 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 ECWS division, and the redundant availability of the normal HVAC System.

B.1 and B.2

If the ECWS division 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 3.7.10.1

Verifying the correct alignment for manual, power operated, and automatic valves in the ECWS flow path provides assurance that the proper flow paths exist for ECWS 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.

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 ECWS components that the ECW pumps will start 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 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. DCD Tier 2, Subsection 9.2.7.

B 3.7 PLANT SYSTEMS

B 3.7.11 Control Room HVAC System (CRHS)

BASES

BACKGROUND

The CRHS consists of control room emergency makeup air cleaning system (CREACS) and control room supply and return system (CRSRS).

The CREACS provides a protected environment from which occupants can control the unit following an uncontrolled released of radioactivity, hazardous chemicals, or smoke. The CRSRS provides air temperature control for the control room.

The CREACS consists of two independent, redundant emergency outside makeup ducts, isolation dampers, and two air cleaning units (ACUs) that recirculate and filter the air in the control room envelope (CRE). Each ACU consists of a moisture separator, two electric heating coils, a prefilter, a high efficiency particulate air (HEPA) filter, an activated carbon adsorber section for removal of gaseous activity (principally iodine), a postfilter, and two fans for filtering the CRE air. Ductwork, valves or dampers, and instrumentation also form part of the system. The prefilters and moisture separator remove any large particles in the air, and any entrained water droplets present to prevent excessive loading of the HEPA filters and carbon absorbers. Continuous operation of each ACU for at least 10 hours per month with the heaters on reduces moisture buildup on the HEPA filters and absorbers. Both the moisture separator and heater are important to the effectiveness of the carbon absorbers. Postfilter follows the absorber section to collect carbon fines and provides backup in case of failure of the main HEPA filter bank.

The CRSRS consists of dual outside air intakes, normal outside makeup duct, isolation dampers, and four air handling units (AHUs) that provides cooling and heating of recirculated CRE air. Each AHU consists of a heating coil, a cooling coil, a fan, and instrumentation and controls to provide for control room temperature control.

The CRE is the area within the confines of the CRE boundary that contains the spaces that control room occupants inhabit to control the unit during normal and accident conditions. This area encompasses the control room and other non-critical areas to which frequent personnel access or continuous occupancy is not necessary in the event of an accident. The CRE is protected during normal operation, natural events, and accident conditions. The CRE boundary is the combination of walls, floor, roof, ducting, doors, penetrations and equipment that physically form the CRE.

BACKGROUND (continued)

The OPERABILITY of the CRE boundary must be maintained to ensure that the inleakage of unfiltered air into the CRE will not exceed the inleakage assumed in the licensing basis analysis of design basis accident (DBA) consequences to CRE occupants.

The CRE and its boundary are defined in the Control Room Envelope Habitability Program.

The CRHS operation to maintain the control room temperature is discussed in DCD Tier 2, Subsection 9.4.1 (Reference 2). Upon receipt of the actuating signal(s), normal makeup air supply to the AHU is isolated, and the stream of ventilation air is recirculated through the filter trains of the CREACS.

The CRHS places the system into either of two separate of operation mode (emergency mode for protection for radiation, or recirculation mode for protection from smoke). Upon receipt of actuation signal of the emergency mode of operation, the unfiltered normal makeup air path is isolated, closes exhaust dampers, and CREACS of the operating division is automatically started. The emergency mode initiates pressurization and filtered ventilation of the air supply to the CRE.

Outside air is filtered, and then added to the air being recirculated from the CRE. Pressurization of the CRE minimizes infiltration of unfiltered air through the CRE boundary from all the surrounding areas adjacent to the CRE boundary.

The air entering the CRE is continuously monitored by radiation detectors. One detector output above the setpoint causes actuation of the emergency radiation state as required.

The CRHS operating at a flow rate of 6,286 cmh (3,700 cfm) pressurizes the control room to about 3.175 mm (0.125 in) water gauge relative to external areas adjacent to the CRE boundary. The CRHS operation in maintaining the CRE habitable is discussed in DCD Tier 2, Section 6.4 (Reference. 1).

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 CRHS is designed in accordance with seismic Category I requirements.

The CRHS is designed to maintain a habitability environment in the CRE for 30 days of continuous occupancy after a design basis accident (DBA) without exceeding a 50 mSv whole body dose or its equivalent to any part of the body.

APPLICABLE SAFETY ANALYSES

The CRHS components are arranged in redundant safety-related ventilation divisions.

The CRHS provides airborne radiological protection for the CRE occupants, as demonstrated by the CRE occupant dose analyses for the most limiting DBA fission product release presented in DCD Tier 2, Chapter 15 (Reference 4).

The location of components and ducting within the CRE ensures an adequate supply of filtered air to all areas requiring access.

The CRHS provides protection from smoke and hazardous chemicals to the CRE occupants. The analysis of hazardous chemicals releases demonstrates that the toxicity limits are not exceeded in the CRE following a hazardous chemical release (Reference. 1). The evaluation of a smoke challenge demonstrates that it will not result in the inability of the CRE occupants to control the reactor either from the control room or from the remote shutdown room (Reference. 3).

The worst case single active failure of a component of the CRHS, assuming a loss of offsite power, does not impair the ability of the system to perform its design function.

The CRHS satisfies Criterion 3 of 10 CFR 50.36 (c)(2)(ii).

LCO

Two independent and redundant divisions of the CRHS are required to be OPERABLE to ensure that at least one is available, if a single failure disables the other division. Total system failure, such as from a loss of both ventilation divisions or from an inoperable CRE boundary, could result in exceeding a dose of 50 mSv to the control room operators in the event of a large radioactive release and in the equipment operating temperature exceeding limits in the event of an accident.

The CRSRS is considered OPERABLE when one AHU that is necessary to maintain MCR temperature is OPERABLE in each division.

These components include the cooling coils and associated temperature control instrumentation. In addition, the CRSRS must be OPERABLE to the extent that air circulation can be maintained.

LCO (continued)

The CREACS is considered OPERABLE when the individual components necessary to limit CRE occupant exposure are OPERABLE in both divisions. A division is considered OPERABLE when:

a. Fan is OPERABLE.

b. HEPA filter and carbon absorber are not excessively restricting flow and are capable of performing their filtration functions.

c. Heater, moisture separator, ductwork, valves, and dampers are OPERABLE and air circulation can be maintained.

In order for the CREACS divisions to be considered OPERABLE, the CRE boundary must be maintained such that the CRE occupant dose from a large radioactive release does not exceed the calculated dose in the licensing basis consequence analyses for DBAs, and that CRE occupants are protected from hazardous chemicals and smoke.

The LCO is modified by a Note allowing the CRE boundary to be opened intermittently under administrative controls. This Note only applies to openings in the CRE boundary that can be rapidly restored to the design condition, such as doors, hatches, floor plugs, and access panels. 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 should be proceduralized and consist of stationing a dedicated individual at the opening who is in continuous communication with the operators in the CRE.

This individual will have to a method to rapidly close the opening and to restore the CRE boundary to a condition equivalent to the design condition when a need for CRE isolation indicated.

APPLICABILITY

In MODES 1, 2, 3, 4, 5, and 6 and during movement of irradiated fuel assemblies, the CRHS must be OPERABLE to ensure that the CRE will remain habitable during and following a DBA and ensure that the control room temperature will not exceed equipment operational requirements following isolation of the control room.

During movement of irradiated fuel, the CRHS must be OPERABLE to cope with the release from a fuel handling accident.

ACTIONS

A.1

With one CRHS division inoperable, action must be taken to restore OPERABLE status within 7 days. In this condition, the remaining OPERABLE CRHS division is adequate to maintain the control room temperature within limits and to perform the CRE occupants protection function. However, the overall reliability is reduced because a single failure in the OPERABLE division could result in less the CRHS 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 division to provide the required capabilities.

B.1, B.2 and B.3

If the unfiltered inleakage of potentially contaminated air past the CRE boundary and into the CRE can result in CRE occupant radiological dose greater than the calculated dose of the licensing basis analyses of DBA consequences (allowed to be up to 50 mSv whole body or its equivalent to any part of the body), or inadequate protection of CRE occupants from hazardous chemicals or smoke, the CRE boundary is inoperable. Actions must be taken to restore an OPERABLE CRE boundary within 92 days.
During the period that the CRE boundary is considered inoperable, action must be initiated to implement mitigating actions to lessen the effect on CRE occupants from the potential hazards of a radiological or chemical event or challenge from the smoke. Actions must be taken within 24 hours to verify that in the event of a DBA, the mitigating actions will ensure that CRE occupant radiological exposures will not exceed the calculated dose of the licensing basis analyses of DBA consequences, and that CRE occupants are protected from hazardous chemical and smoke. These mitigating actions (i.e., actions that are taken to offset the consequences of the inoperable CRE boundary) should be preplanned for implementation upon entry into the condition, regardless of whether entry is intentional or unintentional. The 24-hour Completion Time is reasonable based on the low probability of a DBA occurring during this time period and the use of mitigating actions. The 92-day Completion Time is reasonable based on the determination that the mitigating actions will ensure protection of CRE occupants within analyzed limits while limiting the probability that CRE occupants will have to implement protective measures that could adversely affect their ability to control the reactor and maintain it in a safe shutdown condition in the event of a DBA. In addition, the 92-day Completion Time is a reasonable time to diagnose, plan, and possibly repair and test most problems with the CRE boundary.

ACTIONS (continued)

C.1 and C.2

In MODE 1, 2, 3, or 4, if the inoperable CRHS or the CRE boundary cannot be restore to OPERABLE status 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 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

Required Action D.1 is operated manually.

MODE 5, 6, or during movement of irradiated fuel assemblies, if Required Action A.1 cannot be completed within the required Completion Time, the OPERABLE CRHS division must be immediately placed in the emergency MODE of operation. This action ensures that the remaining division 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 may 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

In MODE 5, 6, or during movement of irradiated fuel assemblies with two CRHS divisions inoperable, or with one or two CREACS divisions inoperable due to an inoperable CRE boundary, action must be taken immediately to suspend activities that could result in a release of radioactivity that may require isolation of CRE. This places the unit in a condition that minimizes the accident risk. This does not preclude the movement of fuel to a safe position.

ACTIONS (continued)

F.1

If both CRHS divisions are inoperable in MODE 1, 2, 3, or 4 for reason other than an inoperable CRE boundary (i.e. Condition B), the CRHS 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.

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 ACU 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 greater than or equal to 10 continuous hours with the heaters energized. 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 CRHS testing is performed in accordance with the ventilation filter testing program (VFTP). The testing is performed in accordance with NRC RG 1.52 (Reference 5). The VFTP includes testing HEPA filter performance, carbon adsorber efficiency, minimum system flow rate, and the physical properties of the activated carbon (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 CRHS division starts and operates on an actual or simulated actuation signal. The 18-month Frequency is consistent with that specified in Reference 5.

SR 3.7.11.4

This SR verifies the OPERABILITY of the CRE boundary by testing for unfiltered air inleakage past the CRE boundary and into the CRE. The details of the testing are specified in the Control Room Envelope Habitability Program.

SURVEILLANCE REQUIREMENTS(continued)

The CRE is considered habitable when the radiological dose to CRE occupants calculated in the licensing basis analyses of DBA consequences is no more than 50 mSv whole body or its equivalent to any part of the body and the CRE occupants are protected from hazardous chemicals and smoke. This SR verifies that the unfiltered air inleakage into the CRE is no greater than the flow rate assumed in the licensing basis analyses of DBA consequences. When unfiltered air inleakage is greater than the assumed flow rate, Condition B must be entered. Required Action B.3 allows time to restore the CRE boundary to OPERABLE status provided mitigating actions can ensure that the CRE remains within the licensing basis habitability limits for the occupants following an accident. Compensatory measures are discussed in NRC RG 1.196, Section C.2.7.3, (Reference 7) which endorses, with exceptions, NEI 99-03, Section 8.4 and Appendix F (Reference 8). These compensatory measures may also be used as mitigating actions as required by Required Action B.2. Temporary analytical methods may also be used as compensatory measures to restore OPERABILITY (Reference 9). Options for restoring the CRE boundary to OPERABLE status include changing the licensing basis DBA consequence analysis, repairing the CRE boundary, or a combination of these actions. Depending upon the nature of the problem and the corrective action, a full scope inleakage test may not be necessary to establish that the CRE boundary has been restored to OPERABLE status.

SR 3.7.11.5

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 CRHS is slow and is not expected over this time period.

REFERENCES

1. DCD Tier 2, Section 6.4.

2. DCD Tier 2, Subsection 9.4.1.

3. DCD Tier 2, Section 9.5.

4. DCD Tier 2, Chapter 15.

5. NRC RG 1.52, Rev. 4, September 2012.

6. NUREG-0800, Section 6.4, Rev. 3, March 2007.

7. NRC RG 1.196, Rev. 1, January 2007.

8. NEI 99-03, “Control Room Habitability Assessment,” June 2001.

9. Letter from Eric J. Leeds (NRC) to James W. Davis (NEI) dated January 30, 2004, “NEI Draft White Paper, Use of Generic Letter 91-18 Process and Alternative Source Terms in the Context of Control Room Habitability.” (ADAMS Accession No. ML040300694).

B 3.7 PLANT SYSTEMS

B 3.7.12 Auxiliary Building Controlled Area Emergency Exhaust System (ABCAEES)

BASES

BACKGROUND

The ABCAEES filters air from the safety-related mechanical equipment rooms including emergency core cooling system (ECCS) equipment rooms during the recirculation phase of a loss-of-coolant accident (LOCA).

The ABCAEES consists of two independent and redundant divisions. Each division includes two emergency exhaust air cleaning units (ACUs), each consisting of a moisture separator, an electric heating coil, a prefilter, a high efficiency particulate air (HEPA) filter, an activated carbon adsorber section for removal of gaseous activity (principally iodines), a postfilter, and a fan. Ductwork, valves or dampers, and instrumentation also form part of the system. The moisture separator removes any entrained water droplets in the air stream to reduce the relative humidity of the air and the prefilter removes any large particles in the air to prevent excessive loading of the HEPA filters and carbon adsorbers. A postfilter follows the adsorber section to collect carbon fines and provide backup in case the HEPA filter bank fails. The system initiates filtered ventilation of the safety-related mechanical equipment rooms following upon receipt of an engineered safety feature actuation signal – safety injection actuation signal (ESFAS-SIAS). In addition, the actuation signal closes isolation dampers downstream of the normal supply air handling units (AHUs) and upstream of the normal exhaust ACUs to prevent in-leakage into the auxiliary building controlled area from outside of the auxiliary building. The normal exhaust ACUs and the normal supply AHUs stop sequently upon the isolation damper close signal.

The ABCAEES is discussed in Subsections 6.5.1, 9.4.5, and 15.6.5 (References 1, 2, and 3, respectively), as it can be used for normal, as well as post-accident, atmospheric cleanup functions.

APPLICABLE SAFETY ANALYSES

The design basis of the ABCAEES 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 recirculation mode.

In such a case, the system limits the radioactive release to within 10 CFR 50.34 limits (Reference 5), or the NRC staff-approved licensing basis (e.g., a specified fraction of 10 CFR 50.34 limits). The analysis of the effects and consequences of a large break LOCA is presented in Reference 3.

The ABCAEES also actuates following a small break LOCA, requiring the unit to go into the recirculation mode of long term cooling and to clean up release 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 can result in a lower efficiency of removal for any gaseous and particulate activity released to the ECCS equipment rooms following a LOCA.

The ABCAEES satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

Two independent and redundant divisions of the ABCAEES are required to ensure that at least one is available, assuming a single failure coincident with a loss of offsite power. Total system failure could result in the atmospheric releases from the safety-related mechanical equipment rooms exceeding the required limits in the event of a DBA.

The ABCAEES is considered OPERABLE when the individual components necessary to maintain the safety-related mechanical equipment rooms filtration are OPERABLE in both divisions. A division is considered OPERABLE when its associated :

a. Fan is OPERABLE.

b. HEPA filter and carbon adsorber are not excessively restricting flow and are capable of performing its filtration functions.

c. Electric heating coil, moisture separator, 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 equipment room boundary (e.g., SI pump rooms, CS pump & miniflow heat exchanger rooms, CS heat exchanger rooms, SC pump & miniflow heat exchanger rooms, SC heat exchanger rooms, mechanical penetration rooms) 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 MCR. This individual will have a method to rapidly close the opening when a need for ECCS equipment room isolation is indicated.

APPLICABILITY

In MODES 1, 2, 3, and 4, the ABCAEES is required to be OPERABLE consistent with the OPERABILITY requirements of the ECCS.

In MODES 5 and 6, the ABCAEES is not required to be OPERABLE, since the ECCS is not required to be OPERABLE.

ACTIONS

A.1

With one ABCAEES division inoperable, the inoperable ABCAEES division must be restored to OPERABLE status within 7 days. In this condition, the remaining OPERABLE division is adequate to perform the ABCAEES function.

The 7-day Completion Time is appropriate because the risk contribution of the system 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 division can provide the required capability.

B.1 and B.2

If the inoperable ABCAEES division cannot be restored to OPERABLE status within the associated Completion Time, the unit must be in a MODE in which overall plant risk is minimized. To achieve this status, the unit must be placed in at least MODE 3 within 6 hours, and in MODE 5 within 36 hours.

ACTIONS (continued)

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 3.7.12.1

Standby systems should be checked periodically to ensure they start and function properly. As the environment and normal operating conditions on this system are not severe, testing each division once every month provides an adequate check on this system. 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 greater than or equal to 10 continuous hours with the heaters energized. The 31-day Frequency is based on the known reliability of equipment and the two division redundancy available.

SR 3.7.12.2

This SR verifies that the required ABCAEES testing is performed in accordance with the Ventilation Filter Testing Program (VFTP). The ABCAEES filter tests are in accordance with NRC RG 1.52 (Reference 4). The VFTP includes testing HEPA filter performance, carbon adsorber efficiency, the minimum system flow rate, and the physical properties of the activated carbon (general use and following specific operations). Specific test frequencies and additional information are discussed in detail in the VFTP.

SR 3.7.12.3

This SR verifies that each ABCAEES division starts and operates on an actual or simulated actuation signal. The 18-month Frequency is consistent with that specified in NRC RG 1.52 (Reference 4).

SR 3.7.12.4

This SR verifies the integrity of the ECCS equipment room enclosure. The ability of the ECCS equipment room to maintain a negative pressure, with respect to potentially uncontaminated adjacent areas, is periodically tested to verify proper function of the ABCAEES. During the post-accident MODE of operation, the ABCAEES is designed to maintain a slightly negative pressure in the ECCS equipment room with respect to adjacent areas to prevent unfiltered LEAKAGE.

SURVEILLANCE REQUIREMENTS (continued)

The ABCAEES is designed to maintain this negative pressure at a flow rate of less than or equal to 5,097 cmh (3,000 cfm) from the auxiliary building controlled area. The 18-month Frequency is consistent with the guidance provided in the NUREG-0800, Subsection 6.5.1 (Reference 6).

This test is conducted with the tests for filter penetration. An 18-month Frequency on a staggered test basis is consistent with other filtration SRs.

REFERENCES

1. DCD Tier 2, Subsection 6.5.1.
2. DCD Tier 2, Subsection 9.4.5.
3. DCD Tier 2, Subsection 15.6.5.
4. NRC RG 1.52, Rev.4, September 2012.
5. 10 CFR 50.34.
6. NUREG-0800, Subsection 6.5.1, Rev. 4, May 2010.

B 3.7 PLANT SYSTEMS

B 3.7.13 Fuel Handling Area Emergency Exhaust System (FHAEES)

BASES

BACKGROUND

The FHAEES filters airborne radioactive particulates from the area of the fuel pool following a fuel handling accident or loss of coolant accident.

The FHAEES consists of two independent, redundant divisions. Each division consists of a moisture separator, an electric heating coil, a prefilter, a high efficiency particulate air (HEPA) filter, an activated carbon absorber section for removal of gaseous activity (principally iodines), postfilter and a fan. Ductwork, valves or dampers, and instrumentation also form part of the system. The prefilters or moisture separators remove any large particles in the air, and any entrained water droplets present, to prevent excessive loading of the HEPA filters and carbon adsorbers. Postfilters follow the absorber section to collect carbon fines and provide backup in case of failure of the main HEPA filter bank. The system initiates filtered ventilation of the fuel handling area following receipt of an engineered safety feature actuation signal-fuel handling area emergency ventilation actuation signal (ESFAS-FHEVAS) or a high radiation signal.

Upon receipt of the ESFAS-FHEVAS or a high radiation signal normal air supply, and normal discharge from the fuel handling area are isolated, and the stream of ventilation air discharges through the FHAEES division.

The FHAEES is discussed in Chapter 9 (Reference 2). It can be used for normal, as well as post-accident, atmospheric cleanup functions.

APPLICABLE SAFETY ANALYSES

The FHAEES is designed to mitigate the consequences of a fuel handling accident in which rods in the fuel assembly are assumed to be damaged. The analysis of the fuel handling accident is given in Reference 3. The design basis accident analysis of the fuel handling accident assumes that only one division of the FHAEES is functional, due to a single failure that disables the other division. The accident analysis accounts for the reduction in airborne radioactive material provided by the remaining one division of this filtration system.

The amount of fission products available for release from the fuel handling area is determined for a fuel handling accident. These assumptions and the analysis follow the guidance provided in NRC RG 1.25 (Reference 5).

LCO

The FHAEES satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii). Two independent and redundant divisions of the FHAEES are required to be OPERABLE to ensure that at least one is available, assuming a single failure of the other division coincident with loss of offsite power. Total system failure could result in the atmospheric release from the fuel handling area exceeding the 10 CFR 50.34 (Reference 6) limits in the event of a fuel handling accident.

The FHAEES is considered OPERABLE when the individual components necessary to control operator exposure are OPERABLE in both divisions. A division is considered OPERABLE when its associated:

a. Fan is OPERABLE.

b. HEPA filter and carbon absorber are not excessively restricting flow and is capable of performing the filtration functions.

c. Heater, moisture separator, ductwork, valves, and dampers are OPERABLE and air circulation can be maintained.

The LCO is modified by a Note allowing the fuel handling area boundary (e.g., SFP cooling heat exchanger rooms, the spent fuel pool, the loading & unloading area) to be opened intermittently under administrative controls. For entry and exit through doors, the administrative control of 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 MCR. This individual will have a method to rapidly close the opening when a need for fuel handling area isolation is indicated.

APPLICABILITY

During movement of irradiated fuel in the fuel handling area, the FHAEES is required to be OPERABLE to mitigate the consequences of a fuel handling accident.

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 a shutdown unnecessarily.

ACTIONS (continued)

A.1

If one FHAEES division is inoperable, action must be taken to restore OPERABLE status within 7 days. During this time period, the remaining OPERABLE division is adequate to perform the FHAEES function. The 7-day Completion Time is reasonable, based on the risk from an event occurring requiring the inoperable FHAEES division and ability of the remaining FHAEES division to provide the required protection.

B.1 and B.2

When Required Action A.1 cannot be completed within the required Completion Time during movement of irradiated fuel assembles in the fuel handling area, the OPERABLE FHAEES division must be started immediately or fuel movement suspended. This action ensures that the remaining division is OPERABLE and that no undetected failures preventing system operation will occur and that any active failures will be readily detected.

If the system is not placed in operation, this action requires suspension of fuel movement which precludes a fuel handling accident. This does not preclude the movement of fuel assemblies to a safe position.

C.1

When two divisions of the FHAEES are inoperable during movement of irradiated fuel assemblies in the fuel building area, action should be taken to place the unit in a condition in which the LCO does not apply. This LCO involves immediately suspending movement of irradiated fuel assemblies in the fuel handling area. This does not preclude the movement of fuel to a safe position.

SURVEILLANCE REQUIREMENTS

SR 3.7.13.1

The standby FHAEES division should be checked periodically to ensure it functions properly. As the environment and normal operating conditions on this system are not severe, testing each division once every month provides an adequate check on this system. Heater operation dries out any moisture accumulated in the carbon from humidity in the ambient air. System with heater must be operated for greater than or equal to 10 continuous hours with the heater energized. The 31-day Frequency is based on the known reliability of the equipment and the two division redundancy available.

SR 3.7.13.2

This SR verifies that the required FHAEES testing is performed in accordance with the ventilation filter testing program (VFTP). The FHAEES filter tests are in accordance with the NRC RG 1.52 (Reference 4). The VFTP includes testing HEPA filter performance, carbon absorber efficiency, minimum system flow rate, and the physical properties of the activated carbon (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 ventilation filter testing division starts and operates on an actual or simulated actuation signal. The 18-month Frequency is specified in NRC RG 1.52.

SR 3.7.13.4

This SR verifies the integrity of the fuel handling area. The ability of the fuel handling area to maintain negative pressure with respect to potentially uncontaminated adjacent areas is periodically tested to verify proper function of the FHAEES. During the post-accident mode of operation, the FHAEES is designed to maintain a slightly negative pressure in the fuel handling area, with respect to adjacent areas, to prevent unfiltered leakage. The FHAEES is designed to maintain this negative pressure at a flow rate of 8,495 cmh (5,000 cfm) from the fuel handling area. The 18-month Frequency is consistent with the guidance provided in NUREG-0800, Subsection 6.5.1 (Reference 7).

This test is conducted with the tests for filter penetration. An 18-month Frequency on a staggered test basis is consistent with other filtration SRs.

REFERENCES

1. DCD Tier 2, Subsection 6.5.1.
2. DCD Tier 2, Subsection 9.4.2.
3. DCD Tier 2, Chapter 15.
4. NRC RG 1.52, Rev. 4, September 2012.
5. NRC RG 1.25, March 1972.
6. 10 CFR 50.34.
7. NUREG-0800, Subsection 6.5.1, Rev. 4, May 2010.

B 3.7 PLANT SYSTEMS

B 3.7.14 Spent Fuel Pool Water Level (SFPWL)

BASES

BACKGROUND

The minimum water level in the spent fuel 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 at their maximum capacity. The water also provides shielding during the movement of spent fuel.

A general description of the spent fuel pool design is found in Subsection 9.1.2 (Reference 1). A general description of the spent fuel pool cooling and cleanup system design is found in Chapter 9.1.3 (Reference 2). The assumptions of the fuel handling accident are found in Chapter 15.7.4 (Reference 3).

APPLICABLE SAFETY ANALYSES

The minimum water level in the spent fuel pool meets the assumptions of the fuel handling accident described in NRC RG 1.195 (Reference 4). The resultant two hour dose to a person at the exclusion area boundary (EAB) is well within the 10 CFR 50.34 (Reference 5) limits.

According to Reference 4, there is 7 m (23 ft) of water between the top of the damaged fuel bundle and the fuel pool surface for a fuel handling accident. With 7 m (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 could be less than 7 m (23 ft) above the top of the fuel bundle and the surface by the width of the bundle. To offset this small non-conservatism, the analysis assumes that all fuel rods fail.

The spent fuel pool water level satisfies LCO SELECTION CRITERION 3.

LCO

The specified water level preserves the assumptions of the fuel handling accident analysis (Reference 3). As such, it is the minimum required for irradiated fuel storage within the spent fuel pool.

BASES

APPLICABILITY

This LCO applies during movement of irradiated fuel assemblies in the spent fuel pool since the potential for a release of fission products exists.

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 spent fuel pool water level is lower than the required level, the movement of irradiated fuel assemblies in the spent fuel 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 3.7.14.1

This SR verifies sufficient spent fuel pool water is available in the event of a fuel handling accident. The water level in the spent fuel 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 plant procedures and are acceptable, based on operating experience.

During refueling operations, the level in the spent fuel pool is in equilibrium with the refueling canal, and the level in the refueling canal is checked daily in accordance with LCO 3.9.6, “Refueling Pool Water Level.”

REFERENCES

1. DCD Tier 2, Subsection 9.1.2.
2. DCD Tier 2, Subsection 9.1.3.
3. DCD Tier 2, Subsection 15.7.4.
4. NRC RG 1.195, May 2003.
5. 10 CFR 50.34.

B 3.7 PLANT SYSTEMS

B 3.7.15 Spent Fuel Pool Boron Concentration

BASES

BACKGROUND	As described in LCO 3.7.16, “Spent Fuel Assembly Storage,” fuel assemblies are stored in the spent fuel racks in accordance with criteria based on initial enrichment and discharge burnup. Although the water in the spent fuel pool is normally borated to greater than or equal to 2,150 ppm, the criteria which limits 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 3.7.16 (e.g., an unirradiated fuel assembly or an insufficiently depleted fuel assembly). This accident is analyzed assuming the case of misloading the fuel pool racks with an unirradiated assembly of maximum enrichment. Another type of postulated accident is associated with a fuel assembly which 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 LCO SELECTION CRITERION 2.
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.

BASES

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.

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 fuel of 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, an immediate verification, by administrative means, of the fuel storage pool fuel locations, to ensure proper locations of the fuel since the last movement of fuel assemblies in the fuel storage pool, 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 3.7.15.1

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 3.7.16 Spent Fuel Assembly Storage

BASES

BACKGROUND

The spent fuel storage facility is designed to store either new (non-irradiated) nuclear fuel assemblies, or burned (irradiated) fuel assemblies in a vertical configuration underwater. The spent fuel pool is sized to store 1,792 irradiated fuel assemblies, which includes storage for five failed fuel assemblies.

The spent fuel storage cells are installed in parallel rows. The center to center nominal distances between fuel assemblies for Region I and Region II are specified in Specification 4.3.1.1. This space and the neutron absorbing material attached to the storage cell are sufficient to maintain a K_{eff} less than 1.0 for spent fuel of original enrichment of up to 5 weight percent.

APPLICABLE SAFETY ANALYSES

The spent fuel storage facility is designed for non-criticality by maintaining sufficient space and using the neutron absorbing material. The spent fuel assembly storage satisfies LCO SELECTION CRITERION 2.

LCO

The restrictions on the placement of fuel assemblies within the spent fuel pool, according to Figure 3.7.16-1 in the accompanying LCO, ensures that the K_{eff} of the spent fuel pool will always remain less than 1.0 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 3.7.16-1 in the accompanying LCO. Fuel assemblies not meeting the criteria of Figure 3.7.16-1 shall be stored in accordance with Specification 4.3.1.1.

APPLICABILITY

This LCO applies whenever any fuel assembly is stored in Region II of the spent fuel pool.

BASES

ACTIONS

A.1

Required Action A.1 is modified by a Note indicating that LCO 3.0.3 is not applied.

When the configuration of fuel assemblies stored in Region II of the spent fuel pool is not in accordance with Figure 3.7.16-1, immediate action must be taken to make the necessary fuel assembly movement to bring the configuration into compliance with Figure 3.7.16-1.

If irradiated fuel assemblies are moved while in MODE 5 or 6, LCO 3.0.3 would not specify any action. If irradiated fuel assemblies are moved 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 3.7.16.1

This SR verifies by administrative means that the initial enrichment and burnup of the fuel assembly is in accordance with Figure 3.7.16-1 in the accompanying LCO. For fuel assemblies in the unacceptable range of Figure 3.7.16-1, performance of this SR will ensure compliance with Specification 4.3.1.1.

REFERENCES

1. DCD Tier 2, Subsection 9.1.1.

B 3.7 PLANT SYSTEMS

B 3.7.17 Secondary Specific Activity

BASES

BACKGROUND

Activity in the secondary coolant results from a steam generator tube leakage of the reactor coolant. Under steady-state conditions, the iodines with relatively short half-lives are main radionuclides in the secondary coolant, and thus is an indicative of current conditions. During a transient, I-131 spike is observed as well as an increased release of some noble gases. Other fission product isotopes, as well as activated corrosion products in lesser amounts, can also be found in the secondary coolant.

A limit on secondary coolant specific activity during power operation minimizes releases to the environment during normal operation, anticipated operational occurrences, and accidents.

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 iodine isotopes have short half-lives, (i.e., less than 20 hours). I-131 with a half-life of 8.04 days concentrates faster than it decays, but does not reach equilibrium because of blowdown and other losses.

If the plant is operating within the LCO limit, the 2-hour exclusion area boundary (EAB) exposure due to an accident is less than a small fraction of the limits in 10 CFR 50.34 (Reference. 1).

BASES

APPLICABLE SAFETY ANALYSES

The accident analysis of the MSLB failure described in DCD Tier 2, Chapter 15 (Reference. 2) assumes the initial secondary coolant specific activity to have a radioactive isotope concentration of 3.7 x 10^3 Bq/g DOSE EQUIVALENT I-131. This assumption is used in the analysis for determining the radiological consequence of a postulated accident. The accident analysis shows that the radiological consequence of a MSLB does not exceed a small fraction of the EAB exposure limits of 10 CFR 50.34.

With the loss of offsite power, the remaining decent steam generator is available for core decay heat dissipation by venting steam to the atmosphere through the main steam safety valves (MSSVs) and main steam atmospheric dump valves (MSADVs). The auxiliary feedwater system supplies the necessary makeup to the steam generator. Venting continues until the reactor coolant temperature and pressure has decreased sufficiently for the shutdown cooling system to be engaged for the cooldown.

In the evaluation of the radiological consequences of a MSLB 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 the MSSVs and MSADVs during the event.

The secondary specific activity satisfies LCO SELECTION CRITERION 2.

LCO

As indicated in the applicable safety analyses, the specific activity limit in the secondary coolant system of less than or equal to 3.7 x 10^3 Bq/g DOSE EQUIVALENT I-131 is required to limit the radiological consequences of a DBA to a small fraction of 10 CFR 50.34.

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.

BASES

APPLICABILITY

In MODES 1, 2, 3 and 4, the limits on secondary specific activity are applied considering the potential secondary steam releases to 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 activity is not required.

ACTIONS

A.1 and A.2

DOSE EQUIVALENT I-131 exceeding the LCO limit is an indication of a problem in the RCS, as well as the possibility of the post-accident doses exceeding the regulatory limit. The plant must be placed in a MODE in which the requirement does not apply if secondary specific activity cannot be restored within limit in the associated Completion Time. This is done by placing the plant in MODE 3 in 6 hours, and MODE 5 in 36 hours. Based on operating experience, the allowed Completion Times are reasonable to reach the required MODES from the full power operation in an orderly manner without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.7.17.1

This SR ensures that the secondary activity is within the limit assumed in the accident analyses. A gamma isotopic analysis of the secondary coolant, which determines DOSE EQUIVALENT I-131, confirms the validity of the accident analysis assumptions as to the source terms in post-accident releases. It also serves to identify and analyze any unusual isotopic concentrations which may indicate changes in reactor coolant activity or LEAKAGE. The 31-day Frequency is sufficient to monitor the level of DOSE EQUIVALENT I-131 and its increasing trends, and to take appropriate ACTIONS to maintain the level below the LCO limit.

REFERENCES

1. 10 CFR 50.34.

2. DCD Tier 2, Chapter 15.

B 3.8 ELECTRICAL POWER SYSTEMS

B 3.8.1 AC Sources – Operating

BASES

BACKGROUND

The Class-1E Electrical Power Distribution System AC power sources consist of the offsite power sources (preferred power sources, normal and alternate), and the onsite standby power sources—two divisions of emergency diesel generators (EDGs), each division consisting of two EDGs (EDG A and EDG C for division I, and EDG B and EDG D for division II). As required by 10 CFR 50, Appendix A, GDC 17 (Reference 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 (divisions) so that 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 EDG.

Offsite power is supplied to the unit switchyard(s) from the transmission network by at least two transmission lines. From the switchyard(s), two electrically and physically separated circuits provide AC power, through [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 DCD Tier 2, Chapter 8 (Reference 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 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.

BASES

BACKGROUND (continued)

The onsite standby power source for each 4.16 kV ESF bus is a dedicated EDG. EDGs [1A, 1B, 1C, and 1D] are dedicated to ESF buses [SW1A, SW1B, SW1C, and SW1D], respectively. An EDG 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 EDG has started, it will automatically tie to its respective bus after offsite power is tripped as a consequence of ESF bus undervoltage or degraded voltage, independent of or coincident with an SI signal. The EDGs 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 strips nonpermanent loads from the ESF bus. When the EDG 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 EDG by automatic load application.

In the event of a loss of preferred power, the ESF electrical loads are automatically connected to the EDGs 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 EDG 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 Trains A, B, C, and D EDGs satisfy the requirements of NRC RG 1.9 (Reference 3). The continuous service rating of each EDGs A and B are 8,700 kW and EDGs C and D are 7,000 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 DCD Tier 2, Chapters 6 (Reference 4) and 15 (Reference 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.

BASES

APPLICABLE SAFETY ANALYSES (continued)

These design 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. The results in maintaining at least one division of the onsite or offsite AC sources OPERABLE during accident conditions in the event of:

a. An assumed loss of all offsite power or all onsite AC power

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 AC Electrical Power Distribution System and separate and independent EDGs 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 DCD Tier 2, Chapter 8, and are part of the licensing basis for the unit.

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 is supplied from the switchyard through the main transformer and the unit auxiliary transformer [TR01M] and powers ESF buses [SW01A] and [SW01C] via its normal feeder breakers. Offsite circuit #2 is normally fed from the switchyard through the standby auxiliary transformer [TR02M] and powers ESF buses [SW01B] and [SW01D] via its normal feeder breakers.

BASES

LCO (continued)

Each EDG must be capable of starting, accelerating to speed and voltage, and connecting to its respective ESF bus on detection of bus undervoltage. This will be accomplished within 17 seconds. Each EDG 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 EDG in standby with the engine hot and EDG in standby with the engine at ambient conditions. Additional EDG capabilities must be demonstrated to meet required Surveillances (e.g., capability of EDG to revert to standby status on a safety injection signal while operating in parallel test mode).

Proper sequencing of loads, including tripping of nonessential loads, is a required function for EDG 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 EDGs, 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.

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 3.0.4b to an inoperable EDG. There is an increased risk associated with entering a MODE or other specified condition in the Applicability with an inoperable EDG and the provisions of LCO 3.0.4b, 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.

A.2

Required Action A.2, which only applies if the division cannot be powered from an offsite source, is intended to provide assurance that an event coincident with a single failure of the associated EDG 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 division.

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 division has no offsite power supplying its loads.

b. A required feature on the other division 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.

ACTIONS (continued)

Discovering no offsite power to one division 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 division that has offsite power, results in starting the Completion Times for the Required Action. A 24-hour Completion Time 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 EDGs are adequate to supply electrical power to Division I and Division II 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 NRC RG 1.93 (Reference 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 EDGs 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 offsite power source remains with an inoperable EDG, 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.

ACTIONS (continued)

B.2

Required Action B.2 is intended to provide assurance that a loss of offsite power, during the period that an EDG is inoperable, does not result in a complete loss of safety function of critical systems. These features are designed with redundant safety related divisions. Redundant required feature failures consist of inoperable features with a division, redundant to the division that has an inoperable EDG.

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 EDG exists.

b. A required feature on the other division is inoperable.

If at any time during the existence of this Condition (one EDG inoperable) a required feature subsequently becomes inoperable, this Completion Time begin to be tracked.

Discovering one required EDG inoperable coincident with one or more inoperable required support or supported features, or both, that are associated with the operable EDG, results in starting the Completion Time for the Required Action. A 4-hour Completion Time 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 EDG 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.

ACTIONS (continued)

B.3.1 and B.3.2

Required Action B.3.1 provides an allowance to avoid unnecessary testing of OPERABLE EDGs. If it can be determined that the cause of the inoperable EDG does not exist on the OPERABLE EDG, SR 3.8.1.2 does not have to be performed. If the cause of inoperability exists on other EDG(s), the other EDG(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 EDG cannot be confirmed not to exist on the remaining EDG(s), performance of SR 3.8.1.2 suffices to provide assurance of continued OPERABILITY of that EDG.

In the event the inoperable EDG 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 GL 84-15 (Reference 7), a time of 24 hours is reasonable to confirm that the OPERABLE EDG(s) is not affected by the same problem as the inoperable EDG.

B.4

According to NRC RG 1.93 (Reference 6), operation may continue in Condition B for a period that should not exceed 72 hours.

In Condition B, the remaining OPERABLE EDG 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.

ACTIONS (continued)

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 division without offsite power (Required Action A.2). The rationale for the reduction to 12 hours is that NRC RG 1.93 (Reference 6) allows a Completion Time of 24 hours for two required offsite circuits inoperable, based upon the assumption that two complete safety divisions 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 divisions.

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.

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 NRC RG 1.93 (Reference 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 can appear to be more severe than other combinations of two AC sources inoperable that involve one or more EDPSs inoperable.

ACTIONS (continued)

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.

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.

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 division, 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 EDG without regard to whether a division is de-energized. LCO 3.8.9 provides the appropriate restrictions for a de-energized division.

According to the NRC RG 1.93 (Reference 6), operation may continue in Condition D for a period that should not exceed 12 hours.

ACTIONS (continued)

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 can 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 the period.

E.1

With division I and division II EDGs 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 very short time could be less than that associated with an immediate controlled shutdown (the immediate shutdown could cause grid instability, which could result in 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.

NRC RG 1.93 (Reference 6), with both divisions inoperable, operation may continue for a period that should not exceed 2 hours.

F.1

The sequencer(s) is an essential support system to the EDG 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 train. 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.

ACTIONS (continued)

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 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.

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 (Reference 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 EDGs are in accordance with the recommendations of NRC RG 1.9 (Reference 3) and NRC RG 1.137 (Reference 9), as addressed in DCD Tier 2, Chapter 8.

Where the SRs discussed herein specify voltage and frequency tolerances, the following is applicable. The minimum steady state output voltage of 3,744 V is 90 % of the nominal 4,160V output voltage. This value, specified in ANSI C84.1-1989 (Reference 10), allows for voltage drop to the terminals of 4,000V motors whose minimum operating voltage is specified as 90 % or 3,600V. It also allows for voltage drops to motors and other equipment down through the 120V level where minimum operating voltage is also usually specified as 80 % of name plate rating. The specified maximum steady state output voltage of 4,576V is equal to the maximum operating voltage specified for 4,000V motors. It ensures that for a lightly loaded distribution system, the voltage at the terminals of 4,000V motors is no more than the maximum rated operating voltages. The specified minimum and maximum frequencies of the EDG 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 NRC RG 1.9 (Reference 3).

<u>SR 3.8.1.1</u>

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 MCR.

SURVEILLANCE REQUIREMENTS (continued)

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 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 2 for SR 3.8.1.7) to indicate that all EDG 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 purpose of SR 3.8.1.2 and 3.8.1.7 testing, the EDGs are started from standby conditions. Standby conditions for an EDG 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 EDG manufacturers recommend a modified start in which the starting speed of EDGs is limited, warmup is limited to this lower speed, and the EDGs 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 the EDG starts from standby conditions and achieves required voltage and frequency within 17 seconds. The 17-second start requirement supports the assumptions of the design basis LOCA analysis in DCD Tier 2, Chapter 15 (Reference 5).

The 17-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, the 17-second start requirement of SR 3.8.1.7 applies.

Since SR 3.8.1.7 requires a 17-second start, it is more restrictive than SR 3.8.1.2 and may be performed in lieu of SR 3.8.1.2.

In addition to the SR requirements, the time for the EDG 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.

SURVEILLANCE REQUIREMENTS (continued)

The 31-day Frequency for SR 3.8.1.2 is consistent with NRC RG 1.9 (Reference 3). The 184-day Frequency for SR 3.8.1.7 is a reduction in cold testing consistent with GL 84-15 (Reference 7). These Frequencies provide adequate assurance of EDG OPERABILITY, while minimizing degradation resulting from testing.

SR 3.8.1.3

This Surveillance verifies that the EDGs 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 EDG is connected to the offsite source.

Although no power factor requirements are established by this SR, the EDG 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 NRC RG 1.9 (Reference 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 EDG at a time in order to avoid common cause failures that may result from offsite circuit or grid perturbations. Note 4 stipulates a prerequisite requirement for performance of this SR. A successful EDG start must precede this test to credit satisfactory performance.

SR 3.8.1.4

This SR provides verification that the level of fuel oil in the day tank is at or above the level at which fuel oil is automatically added. The level is expressed as an equivalent volume in liters (gallons) and is selected to ensure adequate fuel oil for a minimum of 1 hour of EDG operation at full load plus 10 %.

SURVEILLANCE REQUIREMENTS (continued)

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 tank 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 EDG operation. Water can 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 31-day Frequency is established by NRC RG 1.137 (Reference 9). 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 (Reference 11). 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 tanks during or following EDG testing. In such a case, a 31-day Frequency is appropriate. Since proper operation of fuel transfer systems is an inherent part of EDG 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.

SURVEILLANCE REQUIREMENTS (continued)

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 3.8.1.9

Each EDG 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, may result in a trip of the engine. This Surveillance demonstrates the EDG 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 EDG and its horsepower rating is the component cooling water pump with a horsepower (HP) rating of 1250 HP. This Surveillance may be accomplished by:

a. Tripping the EDG output breaker with the EDG carrying greater than or equal to its associated single largest post-accident load while paralleled to offsite power or while solely supplying the bus

b. Tripping its associated single largest post-accident load while the EDG solely supplying the bus

As required by IEEE Std. 308 (Reference 12), 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.

SURVEILLANCE REQUIREMENTS (continued)

The time, voltage, and frequency tolerances specified in this SR are derived from NRC RG 1.9 (Reference 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 EDG. SR 3.8.1.9.1a corresponds to the maximum frequency excursion, while SR 3.8.1.9b and SR 3.8.1.9c 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 NRC RG 1.9 (Reference 3).

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 EDG 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 less than or equal to 0.9. This power factor is representative of the actual inductive loading an EDG 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 less than or equal to 0.9.

SURVEILLANCE REQUIREMENTS (continued)

These conditions occur when grid voltage is high, and the additional field excitation needed to get the power factor to less than or equal 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 could be such that the EDG 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 EDG. In such cases, the power factor shall be maintained as close as practicable to 0.9 without exceeding the EDG 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.

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.

SURVEILLANCE REQUIREMENTS (continued)

SR 3.8.1.10

This Surveillance demonstrates the EDG capability to reject a full load without overspeed tripping or exceeding the predetermined voltage limits. The EDG full load rejection could 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 loads that the EDG experiences following a full load rejection and verifies that the EDG will not trip upon loss of the load. These acceptance criteria provide for EDG damage protection. While the EDG is not expected to experience this transient during an event and continue to be available, this response assures that the EDG 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 NRC RG 1.9 (Reference 3) 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 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 EDG 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 less than or equal to 0.9.

SURVEILLANCE REQUIREMENTS (continued)

This power factor is representative of the actual inductive loading an EDG 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 less than or equal to 0.9. These conditions occur when grid voltage is high, and the additional field excitation needed to get the power factor to less than or equal 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 could be such that the EDG 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 EDG. In such cases, the power factor shall be maintained as close as practicable to 0.9 without exceeding the EDG 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.

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.

SURVEILLANCE REQUIREMENTS (continued)

SR 3.8.1.11

As required by NRC RG 1.9 (Reference 3), this Surveillance demonstrates the as-designed operation of the standby power sources during loss of the offsite power 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 EDG. It further demonstrates the capability of the EDG to automatically achieve the required voltage and frequency within the specified time.

The EDG auto-start time of 17 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 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 EDG 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 EDG 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 18-month Frequency is consistent with the recommendations of NRC RG 1.9 (Reference 3), 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 EDGs during testing. For the purpose of this testing, the EDGs must be started from standby conditions (i.e., engine coolant and oil continuously circulated and temperature maintained consistent with manufacturer recommendations).

SURVEILLANCE REQUIREMENTS (continued)

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 can be taken for unplanned events that satisfy this SR.

SR 3.8.1.12

This Surveillance demonstrates that the EDG automatically starts and achieves the required voltage and frequency within the specified time (17 seconds) from the design basis actuation signal (LOCA signal) and operates for greater than or equal to 5 minutes. The 5-minute period provides sufficient time to demonstrate stability. SR 3.8.1.12d and 3.8.1.12e ensure that permanently connected loads and emergency loads are energized from offsite electrical power system on an ESF signal without loss of offsite power.

The requirement to verify the connection of permanent and auto-connected loads is intended to satisfactorily show the relationship of these loads to the EDG 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, the 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 of connection and loading of loads, testing that adequately shows the capability of the EDG system to perform these functions is acceptable.

SURVEILLANCE REQUIREMENTS (continued)

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 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 EDGs during testing. For the purpose of this testing, the EDGs 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 2. Risk insights or deterministic methods may be used for the assessment. Credit may be taken for unplanned events that satisfy this SR.]

SURVEILLANCE REQUIREMENTS (continued)

SR 3.8.1.13

This Surveillance demonstrates that EDG noncritical protective functions (e.g. high jacket water temperature) are bypassed on a loss of voltage concurrent with an ESF actuation test signal. Noncritical automatic trips are all automatic trips except:

a. Engine overspeed

b. Generator differential current

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 EDG 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 EDG.

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.

This SR is modified by a Note. The reason for the Note is that performing the Surveillance would remove a required EDG from service. 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.

SURVEILLANCE REQUIREMENTS (continued)

----------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.

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

NRC RG 1.9 (Reference 3) requires demonstration that the EDGs can start and run continuously at full load capability for an interval of not less than 24 hours, greater than or equal to 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 EDG. The EDG 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 EDG. Routine overloading could result in more frequent teardown inspections in accordance with vendor recommendations in order to maintain EDG OPERABILITY.

The 18-month Frequency is consistent with the recommendations of NRC RG 1.9 (Reference 3) takes into consideration unit conditions required to perform the Surveillance, and is intended to be consistent with expected fuel cycle lengths.

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 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 3 ensures that the EDG 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 less than or equal to 0.9. This power factor is representative of the actual inductive loading an EDG 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 less than or equal to 0.9. These conditions occur when grid voltage is high, and the additional field excitation needed to get the power factor to less than or equal 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 could be such that the EDG 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 EDG. In such cases, the power factor shall be maintained as close practicable to 0.9 without exceeding the EDG excitation limits.

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 a shutdown from normal Surveillances, and achieve the required voltage and frequency within 17 seconds. The 17-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 NRC RG 1.9 (Reference 3).

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 EDG. Routine overloads could result in more frequent teardown inspection in accordance with vendor recommendations in order to maintain OPERABILITY. This requirement that the diesel has operated for at least 2 hours at full load condition 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 the test. Note 2 allows all EDG 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 NRC RG 1.9 (Reference 3), this Surveillance assures that the manual synchronization and automatic load transfer from the EDG to the offsite source can be made and that the EDG 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 EDG to reload if a subsequent loss of offsite power occurs. The EDG is considered to be in ready to load status when the EDG is at rated speed and voltage, the output breaker is open and can receive an autoclose signal on bus undervoltage, and the load sequence timers are reset.

The 18-month Frequency is consistent with the recommendations of NRC RG 1.9 (Reference 3) and takes into consideration unit conditions required to perform the Surveillance.

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 EDG availability under accident conditions will not be compromised as the result of testing and the EDG 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 EDG running at rated speed and voltage with the EDG output breaker open. These provisions for automatic switchover are required by IEEE Std. 308 (Reference 12), 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 3.8.1.17b is to show that the emergency loading was not affected by the EDG 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.

SURVEILLANCE REQUIREMENTS (continued)

The 18-month Frequency is consistent with the recommendations of NRC RG 1.9 (Reference 3), 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 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 EDGs due to high motor starting currents. The 10 % load sequence time interval tolerance ensures that sufficient time exists for the EDG 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.

SURVEILLANCE REQUIREMENTS (continued)

The 18-month Frequency is consistent with the recommendations of NRC RG 1.9 (Reference 3), 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 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.

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.

SURVEILLANCE REQUIREMENTS (continued)

SR 3.8.1.19

In the event of a DBA coincident with a loss of offsite power, the EDGs are required to supply the necessary power to ESF systems so that the fuel, RCS, and containment design limits are not exceeded.

This Surveillance demonstrates the EDG 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 EDG 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 18-month Frequency 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 EDGs during testing. For the purpose of this testing, the EDGs must be started from standby conditions, that is, with the engine coolant and oil continuously circulated and temperature maintained consistent with manufacturer recommendations for EDGs. 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.

SURVEILLANCE REQUIREMENTS (continued)

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 3.8.1.20

This Surveillance demonstrates that the EDG starting independence has not been compromised. Also, this Surveillance demonstrates that each engine can achieve proper speed within the specified time when the EDGs are started simultaneously.

The 10-year Frequency is consistent with the recommendations of NRC RG 1.9 (Reference 3).

This SR is modified by a Note. The reason for the Note is to minimize wear on the EDG during testing. For the purpose of this testing, the EDGs must be started from standby conditions (i.e., engine coolant and oil continuously circulated and temperature maintained consistent with manufacturer recommendations).

REFERENCES

1. 10 CFR 50, Appendix A, GDC 17.
2. DCD Tier 2, Chapter 8.
3. NRC RG 1.9, Rev. 4, March 2007.
4. DCD Tier 2, Chapter 6.
5. DCD Tier 2, Chapter 15.
6. NRC RG 1.93, Rev. 1, March 2012.
7. Generic Letter 84-15.
8. 10 CFR 50, Appendix A, GDC 18.
9. NRC RG 1.137, Rev. 1, October 1979.
10. ANSI C84.1-1989.
11. ASME OM Code.
12. IEEE Standard 308-2001.

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 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 irradiated fuel.

In general, when the unit is shut down, the Technical Specifications (TS) 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.

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.

BASES

APPLICABLE SAFETY ANALYSES (continued)

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 emergency diesel generator (EDG) 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 division of LCO 3.8.10, “Distribution Systems – Shutdown,” ensures that all required loads are powered from offsite power. Two OPERABLE EDGs, associated with a distribution system division 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 EDG 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 irradiated fuel).

BASES

LCO(continued)

Offsite circuit #1 supplies power from the switchyard to Class 1E ESF buses via the main transformer and the unit auxiliary transformers [TR01M] for division I and [TR02M] for division II. Offsite circuit #2 supplies power from the switchyard to Class 1E ESF buses via the standby auxiliary transformers [TR01N] for division I and [TR02N] for division II.

The EDG 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 17 seconds. The EDG 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 EDG in standby with the engine hot and EDG in standby at ambient conditions.

Proper sequencing of loads, including tripping of nonessential loads, is a required function for EDG OPERABILITY.

In addition, proper sequencer operation is an integral part of offsite circuit OPERABILITY if its inoperability on the ability to start and maintain energized loads required OPERABLE by LCO 3.8.10.

It is acceptable for divisions to be cross tied during shutdown conditions, allowing a single offsite power circuit to supply all required divisions.

APPLICABILITY

The AC sources required to be OPERABLE in MODES 5 and 6 and during movement of irradiated fuel assemblies provide assurance that:

a. Systems to provide adequate coolant inventory makeup are available for the irradiated fuel assemblies.

b. Systems needed to mitigate a fuel handling accident are available.

c. Systems necessary to mitigate the effects of events that can lead to core damage during shutdown are available.

d. Instrumentation and control capability is available for monitoring and maintaining the unit in a cold shutdown condition or refueling condition.

AC power requirements for MODES 1, 2, 3, and 4 are addressed 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 division. Although two divisions may be required by LCO 3.8.10, the remaining division with offsite power available could be capable of supporting sufficient required features to allow continuation of 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, B.1, B.2, and B.3

With the offsite circuit not available to all required divisions, the option would still exist to declare all required features inoperable. Since this option could involve undesired administrative efforts, the allowance for sufficiently conservative ACTIONS is made. With the required EDG inoperable, the minimum required diversity of AC power sources is not available. It is, therefore, required to suspend movement of 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.

ACTIONS(continued)

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 could 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 could 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 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 division is de-energized. LCO 3.8.10 provides the appropriate restrictions for the situation involving a de-energized division.

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 EDG(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 EDG(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 EDG(s) from being paralleled with the offsite power network or otherwise rendered inoperable during performance of SRs, and to preclude deenergizing a required 4,160V 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 EDG. It is the intent that these SRs must still be capable of being met, but actual performance is not required during periods when the EDG and offsite circuit is required to be OPERABLE. Refer to the corresponding Bases for LCO 3.8.1 for a discussion of each SR.

REFERENCE None

B 3.8 ELECTRICAL POWER SYSTEMS

B 3.8.3 Diesel Fuel Oil, Lube Oil, and Starting Air

BASES

BACKGROUND

Each emergency diesel generator (EDG) is provided with a storage tank having a fuel oil capacity sufficient to operate that diesel for a period of 7 days, while the EDG is supplying maximum post loss-of-coolant accident load demand as discussed in Subsection 9.5.4 (Reference 1) and NRC RG 1.137 (Reference 2). The maximum load demand is calculated using the assumption that at least two EDGs are available. This onsite fuel oil capacity is sufficient to operate the EDGs 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 EDG. All outside tanks, pumps, and piping are located underground.

For proper operation of the standby EDGs, it is necessary to ensure the proper quality of the fuel oil. NRC RG 1.137 (Reference 2) addresses the recommended fuel oil practices as supplemented by ANSI N195-1976 (Reference 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 EDG lubrication system is designed to provide sufficient lubrication to permit proper operation of its associated EDG 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 EDG has an air start system with adequate capacity for five successive start attempts on the EDG without recharging the air start receiver(s).

BASES

APPLICABLE SAFETY ANALYSES

The initial conditions of design basis accident (DBA) and transient analyses in DCD Tier 2, Chapter 6 (Reference 4), and in the Chapter 15 (Reference 5), assume engineered safety feature (ESF) systems are OPERABLE. The EDGs 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 LCOs 3.2, "Power Distribution Limits," 3.4, "Reactor Coolant System (RCS)," and 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 EDGs 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. EDG 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 EDG 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 EDG is required to be OPERABLE.

ACTIONS

The ACTIONS Table is modified by a Note indicating that separate Condition entry is allowed for each EDG. This is acceptable, since the Required Actions for each Condition provide appropriate compensatory actions for each inoperable EDG subsystem. Complying with the Required Actions for one inoperable EDG subsystem may allow for continued operation, and subsequent inoperable EDG subsystem(s) are governed by separate Condition entry and application of associated Required Actions.

A.1

In this Condition, the 7-day fuel oil supply for a EDG is not available. However, the Condition is restricted to fuel oil level reductions that maintain at least a 6 day supply. The fuel oil level equivalent to a 6-day supply is [311,486 L (82,286 gal)]. These circumstances could 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 can 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 EDG inoperable. This period is acceptable based on the remaining capacity (greater than or equal to 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

In this Condition, the 7-day lube oil inventory (i.e., sufficient lubricating oil to support 7 days of continuous EDG operation at full load conditions) is not available. However, the Condition is restricted to lube oil volume reductions that maintain at least a 6-day supply. The lube oil inventory equivalent to a 6-day supply is [1,609 L (425 gal)]. 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 EDG inoperable. This period is acceptable based on the remaining capacity (greater than 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.

ACTIONS (continued)

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 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 EDG inoperable. The 7-day Completion Time allows for further evaluation, resampling, and re-analysis of the EDG 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 could involve feed and bleed procedures, filtering, or combinations of these procedures. Even if a EDG start and load was required during this time interval and the fuel oil properties were outside limits, there is a high likelihood that the EDG would still be capable of performing its intended function.

E.1

With starting air receiver pressure less than [40.78 kg/cm^{2}G (580 psig)], sufficient capacity for five successive EDG start attempts does not exist. However, as long as the receiver pressure is greater than [8.79 kg/cm^{2}G (125 psig)], there is adequate capacity for at least one start attempt, and the EDG 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 EDG inoperable. This period is acceptable based on the remaining air start capacity, the fact that most EDG starts are accomplished on the first attempt, and the low probability of an event during this brief period.

ACTIONS (continued)

F.1

With a Required Action and associated Completion Time not met, or one or more EDGs 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 EDG could be incapable of performing its intended function and must be immediately declared inoperable.

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 EDG's operation for 7 days at full load. The fuel oil level equivalent to a 7-day supply is [96,000 gal] when calculated in accordance with References 2 and 3. The required fuel storage volume is determined using the most limiting energy content of the stored fuel. Using the known correlation of diesel fuel oil absolute specific gravity or API gravity to energy content, the required diesel generator output, and the corresponding fuel consumption rate, the onsite fuel storage volume required for 7 days of operation can be determined. SR 3.8.3.3 requires new fuel to be tested to verify that the absolute specific gravity or API gravity is within the range assumed in the diesel fuel oil consumption calculations. 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 EDG. The lube oil inventory equivalent to a 7-day supply is [1,893 L (500 gal)] and is based on the EDG manufacturer consumption values for the run time of the EDG. Implicit in this SR is the requirement to verify the capability to transfer the lube oil from its storage location to the EDG, when the EDG lube oil sump does not hold adequate inventory for 7 days of full load operation without the level reaching the manufacturer recommended minimum level.

SURVEILLANCE REQUIREMENTS (continued)

A 31-day Frequency is adequate to ensure that a sufficient lube oil supply is onsite, since EDG 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 D4057-06 (2011) (Reference 6).

b. Verify in accordance with the tests specified in ASTM D975-12 (Reference 6) that the sample has an absolute specific gravity at 15.6/15.6 °C (60/60 °F) of ≥ 0.83 and ≤ 0.89, or an API gravity at 15.6 °C (60°F) of ≥ 27° and ≤ 39° when tested in accordance with ASTM D1298-99 (2005) (Reference 6), a kinematic viscosity at 40 °C (104 °F) of ≥ 1.9 centistokes and ≤ 4.1 centistokes, and a flash point ≥ 51.7 °C (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 D4176-04 (2009) or a water and sediment content within limits when tested in accordance with ASTM D2709-96 (2011) e1 (Reference 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 D975-12 (Reference 7) are met for new fuel oil when tested in accordance with ASTM D975-12 (Reference 6), except that the analysis for sulfur may be performed in accordance with ASTM D1552-08, ASTM D2622-10, or ASTM D4294-10 (Reference 6).

SURVEILLANCE REQUIREMENTS (continued)

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 EDG operation. This Surveillance ensures the availability of high quality fuel oil for the EDGs.

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 D5452-12 (Reference 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. 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.

SR 3.8.3.4

This Surveillance ensures that, without the aid of the refill compressor, sufficient air start capacity for each EDG is available. The system design requirements provide for a minimum of five engine start cycles without recharging. A start cycle is defined by the EDG 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 MCR, including alarms, to alert the operator to below normal air start pressure.

SURVEILLANCE REQUIREMENTS (continued)

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 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 EDG operation. Water can 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 31-day Surveillance Frequency is established by NRC RG 1.137 (Reference 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. DCD Tier 2, Subsection 9.5.4.
2. NRC RG 1.137, Rev. 1, October 1979.
3. ANSI N195, Rev. 1, 1976.
4. DCD Tier 2, Chapter 6.
5. DCD Tier 2, Chapter 15.
6. ASTM Standards: D4057-06 (2011); D975-12; D1298-99 (2005); D4176-04 (2009); D2709-96 (2011) e1; D1552-08; D2622-10; D4294-10; D5452-12.
7. ASTM Standards, D975-12, 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 (Reference 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 NRC RG 1.6 (Reference 2) and IEEE Std. 308 (Reference 3).

The 125Vdc electrical power system consists of two independent and redundant safety related Class 1E DC electrical power divisions I and II. Each division consists of two independent trains A and C for division I, and trains B and D for division II. In addition, each train consists of one 125Vdc battery, the associated battery charger for each battery, and all the associated control equipment and interconnecting cabling.

Additionally there is one spare battery charger per train, which provides backup service in the event that the preferred battery charger is out of service. If the spare battery charger is substituted for the preferred battery charger, then the requirements of independence and redundancy between division are maintained.

During normal operation, the 125Vdc 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 trains A, B, C, and D DC electrical power subsystems provide the control power for its associated Class 1E AC power loads, 4.16kV switchgear, and 480Vac 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 LCO 3.8.10, “Distribution Systems – Shutdown.”

BACKGROUND (continued)

Each 125Vdc battery is separately housed in a ventilated room apart from its charger and distribution center. 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 other subsystems. There is no sharing between independent Class 1E subsystems, such as batteries, battery chargers, or distribution panels.

Each battery has adequate storage capacity to meet the duty cycle discussed in DCD Tier 2, Chapter 8 (Reference 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 trains A, B, C, and D 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 105Vdc.

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 120Vdc 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 greater than or equal to 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 DCD Tier 2, Chapter 8 (Reference 4).

Each division I and division II 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 DCD Tier 2, Chapter 8 (Reference 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 DCD Tier 2, Chapter 6 (Reference 5) and Chapter 15 (Reference 6), assume that Engineered Safety Feature (ESF) systems are OPERABLE. The DC electrical power system provides normal and emergency DC electrical power for the EDGs, 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

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 subsystem 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 DC electrical power subsystem does not prevent the minimum safety function from being performed (Reference 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.

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 division 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 may have occurred due to the charger inoperability.

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).

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 is now fully capable of supplying the maximum expected load requirement. The 2-amp value is based on returning the battery to 95 % charge and assumes a 5 % design margin for the battery. 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 could 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 72 hours. 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-Class1E battery charger). The 72-hour Completion Time reflects a reasonable time to effect restoration of the qualified battery charger to OPERABLE status.

B.1

Condition B represents one subsystem with one battery inoperable. With one battery inoperable, the DC bus is being supplied by the OPERABLE battery charger. Any event that results in a loss of the AC bus supporting the battery charger will also result in loss of DC to that subsystem. 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 battery. In addition the energization transients of any DC loads that are beyond the capability of the battery charger and normally require the assistance of the battery 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) are identified in Specifications 3.8.4, 3.8.5, and 3.8.6, together with additional specific Completion Times.

ACTIONS (continued)

C.1

Condition C represents one subsystem 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 subsystem. The 2-hour limit is consistent with the allowed time for an inoperable DC distribution subsystem.

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 the 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 NRC RG 1.93 (Reference 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 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 NRC RG 1.93 (Reference 7).

SURVEILLANCE REQUIREMENTS

SR 3.8.4.1

Verifying battery terminal voltage while on float charge for the batteries 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 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 times the number of connected cells or 127.6 V for a 58-cell battery at the battery terminals). This voltage maintains the battery plates in a condition that supports maintaining the grid life. The 7-day Frequency is consistent with manufacturer recommendations.

SR 3.8.4.2

This SR verifies the design capacity of the battery chargers. According to NRC RG 1.32 (Reference 8), 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 ensures that these requirements can be satisfied.

This SR provides two options. One option requires that battery chargers A and B be capable of supplying 800 amps and battery chargers C and D be capable of supplying 1,200 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.

SURVEILLANCE REQUIREMENTS (continued)

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 less than or equal to 2 amps.

The 18-month 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 18-month Surveillance Frequency is consistent with the recommendations of NRC RG 1.32 (Reference 8) and NRC RG 1.129 (Reference 9), 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.

.

BASES

SURVEILLANCE REQUIREMENTS (continued)

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.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 17.
2. NRC RG 1.6, March 10, 1971.
3. IEEE Standard 308-2001.
4. DCD Tier 2, Chapter 8.
5. DCD Tier 2, Chapter 6.
6. DCD Tier 2, Chapter 15.
7. NRC RG 1.93, Rev. 1, March 2012.
8. NRC RG 1.32, Rev. 3, March 2004.
9. NRC RG 1.129, Rev. 2, February 2007.

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 DCD Tier 2, Chapter 6 (Reference 1) and Chapter 15 (Reference 2), assume that Engineered Safety Feature (ESF) systems are OPERABLE. The DC electrical power system provides normal and emergency DC electrical power for the EDGs, 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 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.

c. Adequate DC electrical power is provided to mitigate events postulated during shutdown, such as a fuel handling accident.

In general, when the unit is shut down, the Technical Specifications (TS) 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.

APPLICABLE SAFETY ANALYSES (continued)

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 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 TS 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 TS 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, has found significant risk associated with certain shutdown evolutions. As a result, in addition to the requirements established in the TS, 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 could require the availability of additional equipment beyond that required by the shutdown TS.

The DC sources satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO

The DC electrical power subsystems, each required subsystem consisting of two batteries, one battery charger per battery, and the corresponding control equipment and interconnecting cabling within the subsystem, are required to be OPERABLE to support one subsystem 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).

APPLICABILITY

The DC electrical power sources required to be OPERABLE in MODES 5 and 6, and during movement of irradiated fuel assemblies provide assurance that:

a. Required features needed to mitigate a fuel handling accident are available.

b. Required features necessary to mitigate the effects of events that can lead to core damage during shutdown are available.

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.

ACTIONS (continued)

A.1, A.2 and A.3

Condition A represents one subsystem 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 may have occurred due to the charger inoperability.

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.

ACTIONS (continued)

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 could 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 72 hours. 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 72-hour Completion Time reflects a reasonable time to effect restoration of the qualified battery charger to OPERABLE status.

B.1, B.2.1, B.2.2, and B.2.3

If two subsystems are required by LCO 3.8.10, the remaining subsystem with DC power available could be capable of supporting sufficient systems to allow continuation of 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 can involve undesired administrative efforts. Therefore, the allowance for sufficiently conservative actions is made (i.e., to suspend movement of irradiated fuel assemblies, and operations involving positive reactivity additions) that could result in loss of required SDM (MODE 5) or boron concentration (MODE 6).

ACTIONS (continued)

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 could 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 probability of the occurrence of postulated events. It is further required to immediately initiate action to restore the required DC electrical power subsystems 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 are 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.

BASES

REFERENCES

1. DCD Tier 2, Chapter 6.

2. DCD Tier 2, Chapter 15.

B 3.8 ELECTRICAL POWER SYSTEMS

B 3.8.6 Battery Cell 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.

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 greater than or equal to 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 DCD Tier 2, Chapter 8 (Reference 2).

APPLICABLE SAFETY ANALYSES

The initial conditions of design basis accident (DBA) and transient analyses in DCD Tier 2, Chapter 6 (Reference 3) and Chapter 15 (Reference 4), assume Engineered Safety Feature systems are OPERABLE. The DC electrical power system provides normal and emergency DC electrical power for the EDGs, 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.

BASES

APPLICABLE SAFETY ANALYSES (continued)

This includes maintaining at least one subsystem 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

b. A worst-case single failure

Battery cell parameters satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

Battery cell 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 cell 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 cell parameters are required solely for the support of the associated DC electrical power subsystems. Therefore, battery cell 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 subsystem less than 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 less than 2.07 V and continued operation is permitted for a limited period up to 24 hours.

ACTIONS (continued)

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 no assurance that there is still sufficient battery capacity to perform the intended function and the battery must be declared inoperable immediately.

B.1 and B.2

One or more batteries in one subsystem with float current greater than 2 amps indicates that a partial discharge of the battery capacity has occurred. This could 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 may have occurred due to a temporary loss of the battery charger.

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 subsystem 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 IEEE Std. 450.

ACTIONS (continued)

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 batteries may have to be declared inoperable and the affected cells replaced.

D.1

With one or more batteries in one subsystem 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 subsystem 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 cell 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 subsystem within 2 hours.

F.1

With one or more batteries with any battery cell 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 subsystem 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 might not be sufficient to perform the intended functions. The battery must therefore be declared inoperable immediately.

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 Std. 450 (Reference 1). The 7-day Frequency is consistent with IEEE Std. 450 (Reference 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 Std. 450 (Reference 1)

SURVEILLANCE REQUIREMENTS (continued)

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 31-day Frequency is consistent with IEEE Std. 450 (Reference 1).

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., 45° 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 31-day Frequency is consistent with IEEE Std. 450 (Reference 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.

SURVEILLANCE REQUIREMENTS (continued)

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.

The acceptance criteria for this Surveillance are consistent with IEEE Std. 450 (Reference 1) and IEEE Std. 485 (Reference 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 less than 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 greater than or equal to 100 % of the manufacturer's ratings. Degradation is indicated, according to IEEE Std. 450 (Reference 1), when the battery capacity drops by more than 10 % relative to its capacity on the previous performance test or when it is greater than or equal to 10 % below the manufacturer's rating. These Frequencies are consistent with the recommendations in IEEE Std. 450 (Reference 1).

BASES

SURVEILLANCE REQUIREMENTS (continued)

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.

REFERENCES

1. IEEE Standard 450-2002.
2. DCD Tier 2, Chapter 8.
3. DCD Tier 2, Chapter 6.
4. DCD Tier 2, Chapter 15.
5. IEEE Standard 485-1997.

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 a 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 DCD Tier 2, Chapter 8 (Reference 1).

APPLICABLE SAFETY ANALYSES

The initial conditions of design basis accident (DBA) and transient analyses in DCD Tier 2, Chapter 6 (Reference 2) and Chapter 15 (Reference 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

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).

BASES

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.

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 battery powered inverters (two per division) 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.

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.

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.”

ACTIONS

A.1

With a required inverter inoperable, its associated AC vital bus becomes inoperable until it is re-energized from its Class 1E constant voltage source transformer.

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 bus is re-energized within 2 hours.

BASES

ACTIONS (Continued)

Required Action A.1 allows 24 hours to fix the inoperable inverter and return it to service. The 24-hour limit is based upon NRC RG 1.93 (Reference 4), 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 may entail. When the AC vital bus is powered from its constant voltage transformer, 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 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 MCR that alert the operator to inverter malfunctions.

BASES

REFERENCES

1. DCD Tier 2, Chapter 8.
2. DCD Tier 2, Chapter 6.
3. DCD Tier 2, Chapter 15.
4. NRC RG 1.93, Rev. 1, March 2012.

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 DCD Tier 2, Chapter 6 (Reference 1) and Chapter 15 (Reference 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.

c. Adequate power is available to mitigate events postulated during shutdown, such as a fuel handling accident.

APPLICABLE SAFETY ANALYSES (continued)

In general, when the unit is shut down, the Technical Specification (TS) 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 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 TS 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 TS 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, has found significant risk associated with certain shutdown evolutions. As a result, in addition to the requirements established in the TS, 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 could require the availability of additional equipment beyond that required by the shutdown TS.

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).

BASES

LCO

The inverters 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 inverters provide uninterruptible supply of AC electrical power to the AC vital buses even if the 4.16 kV safety buses are de-energized. OPERABILITY of the inverters 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).

APPLICABILITY

The inverters required to be OPERABLE in MODES 5 and 6 during movement of 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 are available.

c. Systems necessary to mitigate the effects of events that can lead to core damage during shutdown are available.

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 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.

ACTIONS (continued)

A.1, A.2.1, A.2.2, and A.2.3

If two divisions 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 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 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 could 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 inverters 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 is without power or powered from a constant voltage source transformer.

BASES

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 MCR that alert the operator to inverter malfunctions.

REFERENCES

1. DCD Tier 2, Chapter 6.

2. DCD Tier 2, 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 division 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 4.16kV engineered safety feature (ESF) bus, having at least one separate and independent offsite source of power as well as a dedicated onsite emergency diesel generator (EDG) source. Each 4.16kV ESF bus is normally connected to a preferred offsite source. After a loss of the preferred offsite power source to a 4.16kV ESF bus, a transfer to the alternate offsite source is accomplished by using a time delayed bus undervoltage relay. If all offsite sources are unavailable, the onsite EDG supplies power to the 4.16kV ESF bus. Control power for the 4.16kV breakers is supplied from the Class 1E batteries. Additional description of this system can 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 is 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 division 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 125Vdc buses and distribution panels.

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 DCD Tier 2, Chapters 6 (Reference 1) and Chapter 15 (Reference 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 LCO Sections 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.

b. A worst case single failure

The distribution systems satisfy Criterion 3 10 CFR 50.36(c)(2)(ii).

LCO

The required power distribution subsystem 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 division I and division II 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 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.

BASES

LCO (continued)

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 or Class 1E constant voltage transformer.

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 functions. 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 4.16kV 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.

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 division I and division II required AC buses, load centers, motor control centers, or distribution panels (except AC vital buses), in one division inoperable and a loss of function has not occurred, the remaining AC electrical power distribution subsystem 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.

ACTIONS (continued)

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.

Condition A worst scenario is one division without AC power (i.e., no offsite power to the division and the associated EDGs 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 division by stabilizing the unit, and on restoring power to the affected division. 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 division, to the actions associated with taking the unit to shut down within this time limit.

b. The potential for an event in conjunction with a single failure of a redundant component in the division 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 divisions 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.

ACTIONS (continued)

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 or Class 1E constant voltage transformer.

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 division.

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.

ACTIONS (continued)

C.1

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.

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 division and restoring power to the affected division.

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 division.

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 NRC RG 1.93 (Reference 3).

BASES

ACTIONS (continued)

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 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.

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 MCR that alert the operator to subsystem malfunctions.

REFERENCES

1. NRC RG 1.93, Rev. 1, March 2012.

2. DCD Tier 2, Chapter 6.

3. DCD Tier 2, Chapter 15.

Table B 3.8.9-1

AC and DC Electrical Power Distribution Systems

TYPE	VOLTAGE	DIVISION I (1)	DIVISION II (1)
AC safety buses	4,160 V	ESF Bus 1A 1C	ESF Bus 1B 1D
	480 V	Load Centers 1A 1C	Load Centers 1B 1D
	480 V	Motor Control Centers 1A 2A 3A 4A 1C 2C 3C 4C	Motor Control Centers 1B 2B 3B 4B 1D 2D 3D 4D
DC safety buses	125 V	Bus 1A Bus 1C	Bus 1B Bus 1D
AC vital buses	120 V	Bus 1A Bus 1C	Bus 1B Bus 1D

(1) Each division of the AC and DC electric 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 DCD Tier 2, Chapter 6 (Reference 1) and Chapter 15 (Reference 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 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.

c. Adequate power is provided to mitigate events postulated during shutdown, such as a l or a fuel handling accident.

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).

APPLICABILITY

The AC and DC electrical power distribution subsystems required to be OPERABLE in MODES 5 and 6, and during movement of 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 are available.

c. Systems necessary to mitigate the effects of events that can lead to core damage during shutdown are available.

d. Instrumentation and control capability is available for monitoring and maintaining the unit in a cold shutdown or refueling condition.

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.

ACTIONS (continued)

A.1, A.2.1, A.2.2, A.2.3, and A.2.4

Although redundant required features can require redundant divisions of electrical power distribution subsystems to be OPERABLE, one OPERABLE distribution subsystem division could be capable of supporting sufficient required features to allow continuation of irradiated fuel movement. By allowing the option to declare required features associated with an inoperable distribution subsystem inoperable, appropriate restriction are implemented in accordance with the affected distribution subsystems LCO's Required Actions. In many instances, this option can involve undesired administrative efforts. Therefore, the allowance for sufficiently conservative actions is made (i.e., to suspend movement of 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 could 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 (SCS) subsystem could 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 are 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 MCR that alert the operator to subsystem malfunctions.

REFERENCES

1. DCD Tier 2, Chapter 6.
2. DCD Tier 2, Chapter 15.

B 3.9 REFUELING OPERATIONS

B 3.9.1 Boron Concentration

BASES

BACKGROUND

The limit on the boron concentration of the reactor coolant system (RCS), refueling pool and refueling canal during refueling ensures that the reactor remains subcritical during MODE 6. Refueling boron concentration is the soluble boron concentration in the reactor coolant in each of these volumes having direct access to the reactor core during refueling or fuel handling.

The soluble boron concentration offsets the fuel reactivity and is measured by chemical analysis of the reactor coolant. The refueling boron concentration specified in the COLR ensures the k_{eff} of the core will remain less than or equal to 0.95 during fuel handling with control element assemblies (CEAs) and fuel assemblies assumed to be in the most adverse (least negative reactivity) configuration allowed by plant procedures.

10 CFR 50, Appendix A, GDC 26 requires two independent reactivity control systems of different design principles be provided (Reference 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 reactor vessel head is unbolted, the head is slowly raised. The refueling pool and canal are then flooded by pumping borated water from the in-containment refueling water storage tank (IRWST) using the shutdown cooling system (SCS) pump(s).

If additions of boron are required after the vessel has been opened, the CVCS makes the additions through the RCS and open vessel. The pumping action of the shutdown cooling system (SCS) and natural circulation due to thermal driving heads in the vessel and pool mix the added concentrated boric acid with the water in the RCS and the refueling canal.

BASES

BACKGROUND (continued)

The SCS is kept in service during the refueling period to assist in maintaining the boron concentration in the RCS, the refueling canal, and the refueling pool above the COLR limit and to remove core decay heat and provide forced circulation in the RCS. (Refer to LCO 3.9.4, "Shutdown Cooling System (SCS) and Coolant Circulation – High Water Level" and LCO 3.9.5, "Shutdown Cooling System (SCS) and Coolant Circulation – Low Water Level").

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 magnitude of the boron concentration specified in the COLR is based on the nuclear design of each fuel cycle. It is further 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 less than or equal to 0.95 during the refueling operation.

During refueling, the water volume in the spent fuel pool, the transfer canal, the refueling pool, the refueling canal and the reactor vessel form a single mass. As a result, the soluble boron concentration is the same in each of these volumes.

The limiting boron dilution accident occurs in MODE 5 (Reference 2). A detailed discussion of this event is provided in LCO Basis 3.1.2, "SHUTDOWN MARGIN (SDM) – T_{cold} ≤ 99 °C (210 °F)."

The RCS boron concentration satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

The LCO 3.9.1 requires that a minimum boron concentration be maintained while in MODE 6. The boron concentration limit specified in the COLR during fuel handling operations ensures a k_{eff} of less than or equal to 0.95 is maintained. Violation of the LCO could lead to possible inadvertent criticality during MODE 6.

BASES

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} of less than or equal to 0.95. Above MODE 6, LCO 3.1.1, "SHUTDOWN MARGIN (SDM) – T_{cold} > 99 °C (210 °F)," and LCO 3.1.2, "SHUTDOWN MARGIN (SDM) – T_{cold} ≤ 99 °C (210 °F)," ensures that an adequate amount of negative reactivity is available to shut down the reactor and to maintain the reactor 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.

ACTIONS

A.1

Continuation of positive reactivity additions (including actions to reduce boron concentration) is contingent upon maintaining the plant in compliance with the LCO. If the boron concentration of any of the filled portions of the RCS, the refueling canal, or the refueling cavity is less than its limit, all operations involving 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 positive reactivity additions shall not preclude completion of actions to establish a safe condition.

A.2

In addition to immediately suspending positive reactivity additions, boration to restore the concentration must be initiated immediately. In the determination of the required combination of boration flow rate and boron concentration, there is not a unique design basis event which 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 of the RCS 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 completion time depends on the amount of boron which must be injected to reach the required concentration.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.9.1.1

This SR ensures the reactor coolant boron concentration in the RCS, refueling canal and refueling pool is within the COLR limits. The boron concentration in the coolant is determined periodically by chemical analysis. Prior to reconnecting 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. A minimum Frequency of once every 72 hours is a reasonable interval to verify boron concentration. The Surveillance Frequency is based on extensive operating experience and ensures that the boron concentration is checked at adequate intervals.

REFERENCES

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

2 DCD Tier 2, Subsection 15.4.6.

B 3.9 REFUELING OPERATIONS

B 3.9.2 Nuclear Instrumentation

BASES

BACKGROUND

The installed startup range monitors (SRMs) and boron dilution alarm system are used during refueling operations to monitor core reactivity condition. The SRMs are a part of the ex-core neutron flux monitoring system (ENFMS) and related indicators and recorders. These detectors are located external to the reactor vessel and detect neutrons leaking from the core.

The SRMs monitor the neutron flux in counts per second (cps) and cover neutron flux up to 10^5 cps with a 5 % instrument accuracy. Each SRM provides visual indication in the MCR and an audible alarm to alert operators to a possible dilution accident. The ENFMS is designed in accordance with the criteria presented in Reference 1.

APPLICABLE SAFETY ANALYSES

Two OPERABLE SRMs are required to provide a signal to alert the operator to unexpected changes in core reactivity such as a boron dilution accident or an improperly loaded fuel assembly. The safety analysis of the uncontrolled boron dilution accident is described in Reference 2. This analysis shows that the normally available SHUTDOWN MARGIN would be reduced, but that there is sufficient time available for the operator to detect and to terminate the event should it occur.

The SRMs satisfy LCO SELECTION CRITERION 3.

LCO

This LCO requires two OPERABLE SRMs to ensure that redundant monitoring capability is available to detect changes in core reactivity.

APPLICABILITY

In MODE 6 two SRMs must be OPERABLE to determine changes in core reactivity. No other direct means are available to check core reactivity levels.

In MODES 3, 4, and 5, the installed SRMs are required to be OPERABLE by LCO 3.3.14, “Boron Dilution Alarms.”

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, positive reactivity additions 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 could 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, ACTIONS shall be continued until a 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 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 the comparison between channels of the indicated parameter values for each of the functions. 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 12-hour Frequency is consistent with the CHANNEL CHECK Frequency specified similarly for LCO 3.3.1, “Reactor Protection System (RPS) Instrumentation – Operating.”

SR 3.9.2.2

SR 3.9.2.2 is the performance of a CHANNEL CALIBRATION every 18 months. The CHANNEL CALIBRATION for the SRMs consists of obtaining the voltage plateau curves 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.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 13, 26, 28, and 29.

2. DCD Tier 2, Subsection 15.4.6.

B 3.9 REFUELING OPERATIONS

B 3.9.3 Containment Penetrations

BASES

BACKGROUND

During CORE ALTERATIONS or movement of irradiated fuel assemblies within containment, a release of fission product radioactivity within the containment will be restricted from leakage 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 present, therefore, less stringent requirements are needed to isolate the containment from the outside atmosphere. 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 ANSI/ANS56.8-1994 leakage criteria and tests are not required.

The containment structure serves to contain fission product radioactivity which could be released from the reactor core following a Design Basis Accident (DBA), such that offsite radiation exposures are maintained well within the requirements of 10 CFR 100. Additionally, this structure provides radiation shielding from the fission products which could 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 CORE ALTERATIONS or movement of 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 airlocks, 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 Airlocks.” Each airlock has a door at both ends. The doors are normally interlocked to prevent simultaneous opening when containment OPERABILITY is required.

BACKGROUND (continued)

During periods of unit shutdown when containment closure is not required, the door interlock mechanism may be disabled, allowing both doors of an airlock to remain open for extended periods when frequent containment entry is necessary. During CORE ALTERATIONS or movement of irradiated fuel assemblies within containment, containment closure is required; therefore the door interlock mechanism may remain disabled, but one airlock door must remain capable of being closed.

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 System includes two subsystems. The high volume purge subsystem includes two 1219.2 mm (48 in) purge penetrations and two 1219.2 mm (48 in) exhaust penetrations. The low volume purge subsystem includes two 203.2 mm (8 in) purge penetration and two 203.2 mm (8 in) exhaust penetration. During MODES 1, 2, 3, and 4, the two valves in each of the high volume purge and exhaust penetrations are secured in the closed position. The two valves in each of the two low volume purge 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 high volume purge system is used for this purpose and all valves are closed by the ESFAS such as Containment Purge Isolation Actuation Signal(CPIAS) and Containment Isolation Actuation Signal(CIAS) in accordance with LCO 3.3.5, “Engineered Safety Feature Actuation System (ESFAS) Instrumentation.”

The low volume purge system is not used in MODE 6. All four 203.2 mm (8 in) 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 fuel movements (Reference 1).

BASES

APPLICABLE SAFETY ANALYSIS

During CORE ALTERATIONS or movement of irradiated fuel assemblies within containment, the most severe radiological consequences result from a fuel handling accident. The fuel handling accident is a postulated event that involves damage to irradiated fuel (Reference 2). Fuel handling accidents, analyzed in Section 15.7.4, include dropping a single fuel assembly and handling tool or a heavy object onto other irradiated fuel assemblies. The requirements of this LCO and LCO 3.9.6, "Refueling Water Level," and the minimum decay time of 72 hours prior to CORE ALTERATIONS 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 15.7.4, Rev. 1(Reference 3), which defines "well within" 10 CFR 50.34 to 25 % or less of 10 CFR 50.34 values.

Containment penetrations satisfy LCO Selection Criterion 3.

LCO

This LCO limits the consequences of a fuel handling accident 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. For the OPERABLE containment purge penetrations, this LCO ensures that these penetrations are isolable by the Containment Purge System. The OPERABILITY requirements for this LCO ensure that the automatic purge and exhaust valve closure times specified in DCD Tier 2, Chapter 15 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.

APPLICABILITY

The containment penetration requirements are applicable during CORE ALTERATIONS or movement of irradiated fuel assemblies within containment because this is when there is a potential for a 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 CORE ALTERATIONS or movement of irradiated fuel assemblies within containment are not being conducted, the potential for a fuel handling accident does not exist. Therefore, under these conditions no requirements are placed on containment penetration status.

BASES

ACTIONS

A.1 and A.2

With the containment equipment hatch, airlocks, 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 where the isolation function is not needed. This is accomplished by immediately suspending CORE ALTERATIONS and movement of irradiated fuel assemblies within containment. Performance of these actions shall not preclude completion of actions to establish a safe condition.

SURVEILLANCE REQUIREMENTS

SR 3.9.3.1

This SR 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 CORE ALTERATIONS or movement of 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.

SR 3.9.3.2

This SR demonstrates each containment purge and exhaust valve actuates to its isolation position on an actual or simulated actuation signal. The 18-month Frequency maintains consistency with similar ESFAS testing requirements and has been shown to be acceptable through operating experience.

As such, this Surveillance ensures that a postulated fuel handling accident which involves a release of 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 (Reference 3).

REFERENCES

1. GPU Nuclear Safety Evaluation SE-0002000-001, Rev. 0, May 20, 1988.

2. DCD Tier 2, Chapter 15.

3. NUREG-0800, Section 15.7.4, Rev.1, July 1981.

B 3.9 REFUELING OPERATIONS

B 3.9.4 Shutdown Cooling System (SCS) and Coolant Circulation – High Water Level

BASES

BACKGROUND

The main purposes of the shutdown cooling system (SCS) are to remove decay heat and sensible heat from the reactor coolant system (RCS) when RCS pressure and temperature are below approximately 31.6 kg/cm^{2}A (450 psia) and 177°C (350 °F), respectively (Reference 1), to provide sufficient coolant circulation to minimize the effects of a boron dilution accident, and to prevent boron stratification. Heat is transferred from the RCS by circulating reactor coolant through the SCS where the heat is transferred to the component cooling water (CCW) system via the SCS heat exchangers.

The coolant is then returned to the RCS via the DVI nozzle(s). Operation of the SCS for normal cooldown or decay heat removal is manually accomplished from the MCR. The heat removal rate is adjusted by controlling the flow of reactor coolant through the SCS heat exchanger(s) and bypassing the heat exchanger(s). Mixing of the coolant is maintained by this continuous circulation of reactor coolant through the SCS.

APPLICABLE SAFETY ANALYSES

If the reactor coolant temperature is not maintained below 93.3^{o}C (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 SCS is required to be operational in MODE 6, with the water level greater than or equal to 7.0 m (23 ft) above the top of the reactor vessel flange, to prevent this challenge. The LCO does permit de-energizing of the SCS pump for short durations under the condition that the boron concentration is not diluted. This conditional de-energizing of the SCS pump does not result in a challenge to the fission product barrier.

Shutdown Cooling System and Coolant Circulation – High Water Level satisfies LCO Selection Criterion 2.

LCO

Only one SCS train is required for decay heat removal in MODE 6 with water level greater than or equal to 7.0 m (23 ft) above the top of the reactor vessel flange. Only one SCS train is required because the volume of water above the reactor vessel flange provides backup decay heat removal capability. At least one SCS train must be OPERABLE and in operation to:

a. Provide for decay heat removal.

b. Provide mixing of borated coolant to minimize the possibility of a criticality.

c. Provide indication of average reactor coolant temperature.

An OPERABLE train consists of an SCS 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 DVI nozzle(s).

Both SCS pumps may be aligned to the IRWST to support filling or draining the refueling pool or for performance of required testing.

The requirements of this LCO are derived primarily from experience with decay heat removal in shutdown modes of operation. The principal purpose of this specification is to assure the capability to remove decay heat and to control RCS temperature and chemistry.

The LCO is modified by a Note which allows the operating SCS train to be removed from service for up to 1 hour per 8-hour period provided no operation that would cause dilution of the RCS boron concentration is in progress. 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 SCS isolation valve testing. During this 1-hour period, decay heat is removed by natural convection to the large mass of water in the refueling pool.

BASES

APPLICABILITY

One SCS train must be OPERABLE and in operation in MODE 6 with the water level greater than or equal to 7.0 m (23 ft) above the top of the reactor vessel flange to provide decay heat removal. The 7.0 m (23 ft) value was selected because it corresponds to the requirement for fuel movement established by LCO 3.9.6, “Refueling Pool Water Level.” Requirements for the SCS in other MODES are covered by LCOs in Section 3.4, “Reactor Coolant System.”

SCS train requirements in MODE 6 when water level is less than 7.0 m (23 ft) are located in LCO 3.9.5, “SCS and Coolant Circulation – Low Water Level.”

SCS train requirements are met by having one SCS train OPERABLE and in operation except as permitted in the Note to the LCO.

ACTIONS

A.1

If one required SCS train is inoperable or not in operation, there will be no forced circulation to provide mixing to establish uniform boron concentrations. Reduced boron concentrations can occur by the addition of water with lower boron concentration than that contained in the RCS. Therefore, actions which reduce boron concentration shall be suspended immediately.

A.2

If one required SCS train is inoperable or not in operation, 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 7.0 m (23 ft) above the reactor vessel flange provides an adequate available heat sink. Suspending any operation which would increase decay heat load, such as loading a fuel assembly, is a prudent action under this condition.

A.3

If one required SCS train is inoperable or not in operation, immediate actions shall be taken and continued to satisfy the SCS train requirements. With the unit in MODE 6 and the refueling pool water level greater than or equal to 7.0 m (23 ft) above the top of the reactor vessel flange, the completion time of immediate ensures that prompt action is taken to meet the necessary SCS train cooling requirements.

BASES

ACTIONS (continued)

A.4, A.5, A.6.1 and A.6.2

If one required SCS train is inoperable and not 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 airlock must be closed.

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 system.

With SCS train 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 4-hour Completion Time allows fixing of most SCS 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 verifies that the SCS train 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. The 12-hour Frequency is sufficient considering the flow, temperature, pump control, and alarm indications available to the operator to monitor the SCS in the MCR. This Frequency ensures that SCS train operation and flow is checked at adequate intervals.

REFERENCES

1. DCD Tier 2, Chapter 5.

B 3.9 REFUELING OPERATIONS

B 3.9.5 Shutdown Cooling System (SCS) and Coolant Circulation – Low Water Level

BASES

BACKGROUND

The main purposes of the shutdown cooling system (SCS) are to remove decay heat and sensible heat from the reactor coolant system (RCS) when RCS pressure and temperature are below approximately 31.6 kg/cm^{2}A (450 psia) and 177°C (350°F), respectively (Reference 1), to provide sufficient coolant circulation to minimize the effects of a boron dilution accident, and to prevent boron stratification. Heat is transferred from the RCS by circulating reactor coolant through the SCS where the heat is transferred to the component cooling water system (CCWS) via the SCS heat exchangers.

The coolant is then returned to the RCS via the DVI nozzle(s). Operation of the SCS for normal cooldown or decay heat removal is manually accomplished from the MCR. The heat removal rate is adjusted by controlling the flow of reactor coolant through the SCS heat exchanger(s) and bypassing the heat exchanger(s). Mixing of the coolant is maintained by this continuous circulation of reactor coolant through the SCS.

APPLICABLE SAFETY ANALYSES

If the reactor coolant temperature is not maintained below 93.3 °C (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 SCS are required to be OPERABLE, and one train is required to be in operation in MODE 6, with the water level less than 7.0 m (23 ft) above the top of the reactor vessel flange, to prevent this challenge.

SCS and Coolant Circulation – Low Water Level satisfies LCO Selection Criterion 2.

BASES

LCO

Only one SCS train is needed for decay heat removal in MODE 6 with water level less than 7.0 m (23 ft) above the top of the reactor vessel flange. To increase reliability, both SCS trains must be OPERABLE. Additionally, one train of SCS must be in operation in order to:

a. Provide for decay heat removal.

b. Provide mixing of borated coolant to minimize the possibility of a criticality.

c. Provide indication of average reactor coolant temperature.

An OPERABLE SCS train consists of an SCS 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 DVI nozzle(s).

In addition, during REDUCED RCS INVENTORY conditions a containment spray pump in the same train as the operating SCS pump is required to be OPERABLE. The containment spray pump is interchangable with the SCS pump and provides a backup to the operating SCS pump. This requirement ensures forced circulation is available for decay heat removal if the operating SCS pump becomes inoperable for any reason.

The requirements of this LCO are derived primarily from experience with decay heat removal in shutdown modes of operation. The principal purpose of this specification is to assure the capability to remove decay heat and to control RCS temperature, and chemistry with low water level.

Both SCS pumps may be aligned to the IRWST to support filling or draining the refueling pool or for performance of required testing.

APPLICABILITY

Two SCS trains are required to be OPERABLE and one SCS train must be in operation in MODE 6 with the water less than 7.0 m (23 ft) above the top of the reactor vessel flange to provide decay heat removal. Requirements for the SCS in other MODES are covered by LCOs in Section 3.4, Reactor Coolant System. MODE 6 requirements with water level greater than or equal to 7.0 m (23 ft) above the reactor vessel flange are covered in LCO 3.9.4, “SCS and Coolant Circulation – High Water Level.”

ACTIONS

A.1 and A.2

With one SCS train inoperable and the other SCS train operating, actions shall be taken and continued until the SCS train is restored to OPERABLE status or to establish water level of greater than 7.0 m (23 ft) above the reactor vessel flange. At that point, the Applicability will change to that of LCO 3.9.4, “SCS and Coolant Circulation – High Water Level,” and only one SCS train is required to be OPERABLE and in operation. With the unit in MODE 6, immediate corrective actions must be taken.

B.1

If no SCS train is in operation or no SCS trains are OPERABLE, there will be no forced circulation to provide mixing to establish uniform boron concentrations. Reduced boron concentrations can occur by the addition of water with lower boron concentration than that contained in the RCS. Therefore, actions which reduce boron concentration shall be suspended immediately.

B.2

With no SCS train in operation or with both SCS trains inoperable, actions shall be initiated immediately and continued without interruption to restore one SCS train to OPERABLE status and operation. As the unit is in Conditions A and B concurrently, the restoration of two OPERABLE SCS trains and one operating SCS train should be accomplished as quickly as possible. With at least one SCS train operable, water level can be raised greater than or equal to 7.0 m (23 ft) above the reactor vessel flange and the applicability will change to that of LCO 3.9.4, “SCS and Coolant Circulation – High Water Level,” and only one SCS train is required.

B.3

If no SCS train is in operation or no SCS trains are OPERABLE and the plant is in REDUCED RCS INVENTORY conditions the action requires to immediately initiate action to raise RCS level to greater than EL 38.7 m (127 ft). The immediate Completion Time reflects the importance of maintaining operation for decay heat removal and prevent a boron dilution event.

ACTIONS (continued)

C.1, C.2 and C.3

If the containment spray pump in the same train as an operating SCS train is inoperable, action must be initiated to place the alternate SCS train in operation (if the containment spray pump in the alternate SCS train is OPERABLE) immediately. Also, SCS performance must be monitored every 30 minutes and the inoperable containment spray pump must be restored to OPERABLE condition within 48 hours.

D.1

If the containment spray pump cannot be restored within 48 hours, RCS level must be raised to greater than 38.7 m (127 ft) within 6 hours. This will place the plant in a conservative position with respect to providing decay heat removal.

E.1, E.2, E.3.1 and E.3.2

If no SCS train or CSP is OPERABLE and 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 airlock must be closed.

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 system.

With SCS train 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 4-hour Completion Time allows fixing of most SCS problems and is reasonable, based on the low probability of the coolant boiling in that time.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.9.5.1

This Surveillance verifies that the SCS train is operating and circulating reactor coolant. The flow rate is determined by the flow rate necessary to provide sufficient decay heat removal and to prevent thermal and boron stratification in the core. In addition, this surveillance demonstrates that the other SCS train is OPERABLE.

In addition, during operation of the SCS train with the water level in the vicinity of the reactor vessel nozzles, the SCS train flow rate determination must also consider the SCS pump suction requirements. The 12-hour Frequency is sufficient considering the flow, temperature, pump control, and alarm indications available to the operator to monitor the SCS system in the MCR. This Frequency ensures that flow is checked and temperature monitored at adequate intervals.

Verification that the required trains are OPERABLE and in operation ensures that trains can be placed in operation as needed, to maintain decay heat and retain forced circulation. The 12-hour Frequency 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 SCS pump can be placed in operation, if needed, to maintain decay heat removal and reactor coolant circulation.

Verification is performed by ensuring correct breaker alignment and indicated power available to the required pumps. The 7-day Frequency is considered reasonable in view of other administrative controls available and has been shown to be acceptable by operating experience.

SR 3.9.5.3

Verification of the correct breaker alignment and indicated power available to the operable CS pump ensures that the CS pump will be able to remove heat from the RCS in the event of a power failure to the operating SCS train. The 24-hour Frequency is based on operating experience.

REFERENCES

1. DCD Tier 2, Chapter 5.

B 3.9 REFUELING OPERATIONS

B 3.9.6 Refueling Pool Water Level

BASES

BACKGROUND

The movement of irradiated fuel assemblies or performance of CORE ALTERATIONS, except during latching and unlatching of control rod drive shafts, within containment requires a minimum water level of 7 m (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 (References 1 and 2). Sufficient iodine activity would be retained to limit offsite doses from the accident to under 25 % of 10 CFR 50.34 limits, as provided by the guidance of Reference 3.

APPLICABLE SAFETY ANALYSES

During CORE ALTERATIONS and during movement of irradiated fuel assemblies, the water level in the refueling pool and refueling canal is an initial condition design parameter in the analysis of the fuel handling accident in containment postulated by NRC RG 1.183 (Reference 1). A minimum water level of 7 m (23 ft) allows a decontamination factor of 200 to be used in the accident analysis for iodine. This relates to the assumption that 99.5 % of the total iodine released from the pellet to cladding gap of all the dropped fuel assembly rods is retained by the refueling pool water.

The fuel handling accident analysis inside containment is described in Reference 2. With a minimum water level of 7 m (23 ft) and a minimum decay time of 72 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 (Reference 4).

LCO

Refueling water level satisfies LCO SELECTION CRITERION 4. A minimum refueling water level of 7 m (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 (Reference 3).

BASES

APPLICABILITY

LCO 3.9.6 is applicable during CORE ALTERATIONS, except during latching and unlatching of control rod drive shafts, and when moving irradiated fuel assemblies within containment. 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 3.7.14, “Spent Fuel Pool Water Level.”

ACTIONS

A.1 and A.2

With a water level of less than 7 m (23 ft) above the top of the reactor vessel flange, all CORE ALTERATIONS and operations involving movement of irradiated fuel assemblies shall be suspended immediately to ensure a fuel handling accident cannot occur. The suspension of fuel CORE ALTERATIONS and movement shall not preclude completion of movement to a safe position.

A.3

In addition to immediately suspending CORE ALTERATIONS or movement of irradiated fuel, actions to restore refueling pool water level must be initiated immediately.

SURVEILLANCE REQUIREMENTS

SR 3.9.6.1

Verification of a minimum refueling pool water level of 7 m (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, mitigates the consequences of a postulated fuel handling accident inside containment which results in damaged fuel rods (Reference 2).

The 24-hour Frequency ensures that the water is at the required level and is considered adequate due to the large volume of water and the normal procedural controls of valve positions, significant unplanned level changes are unlikely.

REFERENCES

1. NRC RG 1.183, July 2000.
2. DCD Tier 2, Subsection 15.7.4.
3. NUREG-0800, Section 15.0.1, July 2007.
4. 10 CFR 50.34.