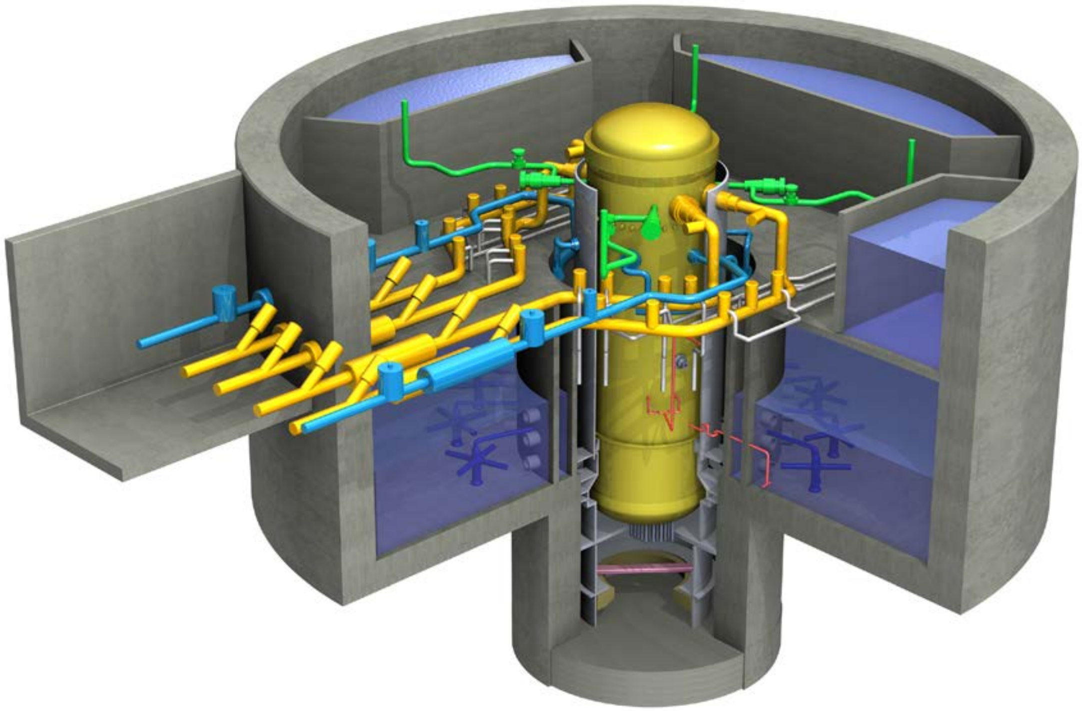
GE Hitachi Nuclear Energy

26A6642BT
Revision 10
April 2014



ESBWR Design Control Document
Generic Technical Specifications

Chapter 16B
Bases

TABLE OF CONTENTS / REVISION SUMMARY Revision - Date

TABLE OF CONTENTS / REVISION SUMMARY Revision - Date

TABLE OF CONTENTS / REVISION SUMMARY Revision - Date

B 2.0 SAFETY LIMITS (SLs)

B 2.1.1 Reactor Core SLs

BASES

BACKGROUND

GDC 10 (Ref. 1) requires, and SLs ensure, that specified acceptable fuel design limits are not exceeded during steady state operation, normal operational transients, and anticipated operational occurrences (AOOs).

Because fuel damage is not directly observable, a stepback approach is used to establish the SL specified in Specification 2.1.1.2. The fuel cladding is one of the physical barriers that separate the radioactive materials from the environs. The integrity of this cladding barrier is related to its relative freedom from perforations or cracking. Although some corrosion or use related cracking may occur during the life of the cladding, fission product migration from this source is incrementally cumulative and continuously measurable. Fuel cladding perforations, however, can result from thermal stresses, which occur from reactor operation significantly above design conditions.

While fission product migration from cladding perforation is just as measurable as that from use related cracking, the thermally caused cladding perforations signal a threshold beyond which still greater thermal stresses may cause gross, rather than incremental, cladding deterioration. These conditions represent a significant departure from the condition intended by design for planned operation. Since the parameters that result in fuel damage are not directly observable during reactor operation, the thermal and hydraulic conditions that result in the onset of transition boiling have been used to mark the beginning of the region in which fuel damage could occur.

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

BASES

APPLICABLE SAFETY ANALYSES

The fuel cladding must not sustain damage as a result of normal operation and AOOs. To ensure damage does not occur, the Fuel Cladding Integrity Safety Limit (FCISL) is established as greater than 99.9% of the fuel rods in the core would be expected to avoid boiling transition. The Reactor Protection System setpoints (LCO 3.3.1.1, "Reactor Protection System (RPS) Instrumentation"), in combination with other LCOs, are designed to prevent any anticipated combination of transient conditions for Reactor Coolant System water level, pressure, and THERMAL POWER level that would result in reaching the FCISL limit. The Safety Limit MCPR (SLMCPR) is a lower bound on the steady-state MCPR that ensures greater than 99.9% of the fuel rods in the core would be expected to avoid boiling transition.

2.1.1.1 Fuel Cladding Integrity

GE14 critical power correlations are applicable for all critical power calculations at pressures > 4.72 MPa (685 psig) (Ref. 2). However, for operation at low pressures, and low-power operation at higher pressures up to 25% RTP at rated pressure, such as may be seen during startup or shutdown, another basis applies: The full scale thermal hydraulic testing of prototypical ESBWR fuel assemblies at low pressure was performed at very low flows and over a range of inlet temperatures and pressures representative of startup conditions and the onset of Boiling Transition observed. The critical bundle powers at which the onset of Boiling Transition occurred in these experiments was a factor of 3, or more, higher than achievable bundle powers in reactor during low pressure, low power operation even when very conservative assumptions on reactor conditions are made. Adequate heat transfer is assured during low pressure and low power operation, including startup and operation up to 25% RTP at rated pressure.

2.1.1.2 FCISL and SLMCPR

The FCISL is set such that no significant fuel damage is calculated to occur for AOOs. Although it is recognized that the onset of transition boiling would not result in damage to BWR fuel rods, a calculated fraction of rods expected to avoid boiling transition has been adopted as a convenient limit. The steady-state and transient uncertainties and the uncertainties in monitoring and simulating the core operating state are incorporated by the statistical model that calculates the fraction of rods. Therefore, an operating limit MCPR is defined such that the FCISL is not violated during normal operations and AOOs, considering the power distribution within the core and all uncertainties.

BASES

APPLICABLE SAFETY ANALYSES (continued)

The probability of the occurrence of boiling transition is determined using the approved General Electric Critical Power correlations. Details of the FCISL calculation process are given in References 2, 3, 4, and 5. Reference 2 also describes the methodology for determining the transient uncertainties and the process for calculating the operating limit MCPR, and the steady state uncertainties used in the statistical analysis.

The Safety Limit MCPR (SLMCPR) is a lower bound on the steady-state MCPR. Details of the SLMCPR calculation process are given in Reference 2.

2.1.1.3 Reactor Vessel Water Level

During MODES 1 and 2, the reactor vessel water level is required to be above the top of the active fuel to provide core cooling capability. With fuel in the reactor vessel during periods when the reactor is shut down, consideration must be given to water level requirements due to the effect of decay heat. If the water level should drop below the top of the active irradiated fuel during this period, the ability to remove decay heat is reduced. This reduction in cooling capability could lead to elevated cladding temperatures and clad perforation in the event that the water level drops below the top of the active irradiated fuel. The reactor vessel water level SL has been established at the top of the active irradiated fuel to provide a point that can be monitored.

SAFETY LIMITS

The reactor core SLs are established to protect the integrity of the fuel clad barrier to the release of radioactive materials to the environs. SL 2.1.1.1 and SL 2.1.1.2 ensure that the core operates within the fuel design criteria. SL 2.1.1.3 ensures that the reactor vessel water level is greater than the top of the active irradiated fuel in order to prevent elevated clad temperatures and resultant clad perforations.

APPLICABILITY

SLs 2.1.1.1, 2.1.1.2, and 2.1.1.3 are applicable in all MODES.

BASES

SAFETY LIMIT VIOLATIONS

Exceeding a SL may cause fuel damage and create a potential for radioactive releases in excess of 10 CFR 52.47(a)(2)(iv) (Ref. 6). Therefore, it is required to insert all insertable control rods and restore compliance with the SL within 2 hours. The 2 hour Completion Time ensures that the operators take prompt remedial action and the probability of an accident occurring during this period is minimal.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 10.
2. NEDC-33237P-A, GE14 for ESBWR - Critical Power Correlation, Uncertainty, and OLMCPR Development, Revision 5, September 2010.
3. NEDE-10958-PA, General Electric Thermal Analysis Basis Data, Correlation and Design Application, January 1977.
4. NEDC-33083P-A, TRACG Application for ESBWR, Revision 1, September 2010.
5. NEDC-32601P-A, Methodology and Uncertainties for Safety Limit MCPR Evaluations, August 1999.
6. 10 CFR 52.47(a)(2)(iv).

B 2.0 SAFETY LIMITS (SLs)

B 2.1.2 Reactor Coolant System (RCS) Pressure SL

BASES

BACKGROUND

The SL on reactor vessel bottom pressure protects 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. Establishing an upper limit on reactor vessel bottom pressure ensures continued RCS integrity. According to 10 CFR 50, Appendix A, GDC 14, "Reactor Coolant Pressure Boundary," and GDC 15, "Reactor Coolant System Design" (Ref. 1), the reactor coolant pressure boundary (RCPB) shall be designed with sufficient margin to ensure that the design conditions are not exceeded during normal operation and anticipated operational occurrences (AOOs).

During normal operation and AOOs, RCS pressure is limited from exceeding the design pressure by more than 10%, in accordance with Section III of the ASME Code (Ref. 2). To ensure system integrity, all RCS components are hydrostatically tested at 125% of design pressure, in accordance with ASME Code requirements, prior to initial operation when there is no fuel in the core. Any further hydrostatic testing with fuel in the core may be done under LCO 3.10.1, "Inservice Leak and Hydrostatic Testing Operation." Following inception of unit operation, RCS components shall be pressure tested in accordance with the requirements of ASME Code, Section XI (Ref. 3).

Overpressurization of the RCS could result in a breach of the RCPB, reducing the number of protective barriers designed to prevent radioactive releases from exceeding the limits specified in 10 CFR 52.47(a)(2)(iv) (Ref. 4). If this occurred in conjunction with a fuel cladding failure, the number of protective barriers designed to prevent radioactive releases from exceeding the limits would be reduced.

APPLICABLE SAFETY ANALYSES

The RCS safety relief valves and the Reactor Protection System Scram settings are established to ensure that the RCS pressure SL will not be exceeded.

The RCS pressure SL has been selected such that it is at a pressure below which it can be shown that the integrity of the system is not endangered. The reactor pressure vessel is designed to ASME, Boiler and Pressure Vessel Code, Section III, 2001 Edition, including Addenda

BASES

APPLICABLE SAFETY ANALYSES (continued)

through 2003 (Ref. 5), which permits a maximum pressure transient of 110% of the design pressure of 8.618 MPaG (1250 psig). Therefore, the SL is 9.481 MPaG (1375 psig) at the lowest elevation of the RCS. The RCS pressure SL is selected to be the lowest transient overpressure allowed by the applicable codes.

SAFETY LIMITS

The maximum transient pressure allowable in the RCS pressure vessel under the ASME Code, Section III, is 110% of design pressure. The maximum transient pressure allowable in the RCS piping, valves, and fittings is 110% of design pressures of 8.618 MPaG (1250 psig). The most limiting of these allowances is the 110% of the RCS design pressure; therefore, the SL on maximum allowable RCS pressure is established at 9.481 MPaG (1375 psig) at the lowest elevation of the RCS.

APPLICABILITY

SL 2.1.2 applies in all MODES.

SAFETY LIMIT VIOLATIONS

Exceeding the RCS pressure SL may cause immediate RCS failure and create a potential for radioactive releases in excess of 10 CFR 52.47(a)(2)(iv) (Ref. 4). Therefore, it is required to insert all insertable control rods and restore compliance with the SL within 2 hours. The 2 hour Completion Time ensures that the operators take prompt remedial action and also assures that the probability of an accident occurring during this period is minimal.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 14 and GDC 15.
2. ASME, Boiler and Pressure Vessel Code, Section III, Article NB-7000.
3. ASME, Boiler and Pressure Vessel Code, Section XI, Article IW-5000.
4. 10 CFR 52.47(a)(2)(iv).
5. ASME, Boiler and Pressure Vessel Code, 2001 Edition, Addenda, 2003.

B 3.0 LIMITING CONDITION FOR OPERATION (LCO) APPLICABILITY

BASES

LCOs	LCO 3.0.1 through LCO 3.0.7 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.

BASES

LCO 3.0.2 (continued)

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

The nature of some Required Actions of some Conditions necessitates that, once the Condition is entered, the Required Actions must be completed even though the associated Conditions no longer exist. The individual LCO's ACTIONS specify the Required Actions where this is the case. An example of this is in LCO 3.4.4, “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/divisions/trains of a safety function are inoperable and limits the time conditions exist which may result in LCO 3.0.3 being entered. Individual Specifications may specify a time limit for performing an SR when equipment is removed from service or bypassed for testing. In this case, the Completion Times of the Required Actions are applicable when this time limit expires, if the equipment remains removed from service or bypassed.

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

LCO 3.0.3

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

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.

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

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

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

a. The LCO is now met;

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

LCO 3.0.3 (continued)

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

The time limits of LCO 3.0.3 allow 37 hours for the unit to be in MODE 5 when a shutdown is required during MODE 1 operation. If the unit is in a lower MODE of operation when a shutdown is required, the time limit for reaching the next lower MODE applies. If a lower MODE is reached in less time than allowed, however, the total allowable time to reach MODE 5, or other applicable MODE, is not reduced. For example, if MODE 2 is reached in 2 hours, then the time allowed for reaching MODE 3 is the next 11 hours, because the total time for reaching MODE 3 is not reduced from the allowable limit of 13 hours. Therefore, if remedial measures are completed that would permit a return to MODE 1, a penalty is not incurred by having to reach a lower MODE of operation in less than the total time allowed.

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

Exceptions to LCO 3.0.3 are provided in instances where requiring a unit shutdown, in accordance with LCO 3.0.3, would not provide appropriate remedial measures for the associated condition of the unit. An example of this is in LCO 3.7.5, “Fuel Pool Water Level and Temperature.” LCO 3.7.5 has an Applicability of “During movement of irradiated fuel assemblies in the associated fuel storage pool” and “When irradiated fuel assemblies are stored in the associated fuel storage pool.” Therefore, this LCO can be applicable in any or all MODES. If the LCO and the Required Actions of LCO 3.7.5 are not met while in MODE 1, 2, 3, or 4, there is no safety benefit to be gained by placing the unit in a shutdown condition. The Required Actions of LCO 3.7.5 of “Suspend movement of irradiated fuel assemblies in the associated fuel storage pool(s)” and “Initiate action to restore water level and temperature to within limit” are the appropriate Required Actions 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 allows placing the unit in a MODE or other specified condition stated in that Applicability (e.g., the Applicability desired to be entered) when unit conditions are such that the requirements of the LCO would not be met, in accordance with LCO 3.0.4.a, LCO 3.0.4.b, or LCO 3.0.4.c.

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

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

The risk assessment may use quantitative, qualitative, or blended approaches, and the risk assessment will be conducted using the plant program, procedures, and criteria in place to implement 10 CFR 50.65(a)(4), which requires that risk impacts of maintenance activities to be assessed and managed. The risk assessment, for the purposes of LCO 3.0.4.b, must take into account all inoperable Technical Specification equipment regardless of whether the equipment is included in the normal 10 CFR 50.65(a)(4) risk assessment scope. The risk assessments will be conducted using the procedures and guidance endorsed by Regulatory Guide 1.182, “Assessing and Managing Risk Before Maintenance Activities at Nuclear Power Plants.” Regulatory Guide 1.182 endorses the guidance in Section 11 of NUMARC 93-01, “Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants.” These documents address general guidance for conduct of the risk assessment, quantitative and qualitative guidelines for establishing risk management actions, and example risk management actions. These include actions to plan and conduct other activities in a manner that controls overall risk, increased risk awareness by shift and management personnel, actions to reduce the duration of the condition,

BASES

LCO 3.0.4 (continued)

actions to minimize the magnitude of risk increases (establishment of backup success paths or compensatory measures), and determination that the proposed MODE change is acceptable. Consideration should also be given to the probability of completing restoration such that the requirements of the LCO would be met prior to the expiration of ACTIONS Completion Times that would require exiting the Applicability.

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

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

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

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

BASES

LCO 3.0.4 (continued)

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 any unit shutdown. In this context, a unit shutdown is defined as a change in MODE or other specified condition in the Applicability associated with transitioning from MODE 1 to MODE 2, MODE 2 to MODE 3, MODE 3 to MODE 4, and MODE 4 to MODE 5.

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

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

LCO 3.0.5

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

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

b. The OPERABILITY of other equipment.

BASES

LCO 3.0.5 (continued)

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

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

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

LCO 3.0.6

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

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

BASES

LCO 3.0.6 (continued)

eliminated by providing all the actions that are necessary to ensure the plant 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.

Specification 5.5.8, “Safety Function Determination Program (SFDP),” ensures loss of safety function is detected and appropriate actions are taken. Upon entry into LCO 3.0.6, an evaluation shall be made to determine if loss of safety function exists. Additionally, other limitations, remedial actions, or compensatory actions may be identified as a result of the support system inoperability and corresponding exception to entering supported system Conditions and Required Actions. The SFDP implements the requirements of LCO 3.0.6.

Cross division/train checks to identify a loss of safety function for those support systems that support safety systems are required. The cross division/train check verifies that the supported systems of the redundant OPERABLE support system are OPERABLE, thereby ensuring safety function is retained.

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.

This loss of safety function does not require the assumption of additional single failures or loss of offsite power. Since operations are being restricted in accordance with the ACTIONS of the support system, any resulting temporary loss of redundancy or single failure protection is taken into account.

BASES

LCO 3.0.6 (continued)

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

LCO 3.0.7

There are certain special tests and operations required to be performed at various times over the life of the unit. These special tests and operations are necessary to demonstrate select unit performance characteristics, to perform special maintenance activities, and to perform special evolutions. Special Operations LCOs in Section 3.10 allow specified TS requirements to be changed to permit performances of these special tests and operations, which otherwise could not be performed if required to comply with the requirements of these TS. Unless otherwise specified, all the other TS requirements remain unchanged. This will ensure all appropriate requirements of the MODE or other specified condition not directly associated with or required to be changed to perform the special test or operation will remain in effect.

The Applicability of a Special Operations LCO represents a condition not necessarily in compliance with the normal requirements of the TS. Compliance with Special Operations LCOs is optional. A special operation may be performed either under the provisions of the appropriate Special Operations LCO or under the other applicable TS requirements. If it is desired to perform the special operation under the provisions of the Special Operations LCO, the requirements of the Special Operations LCO shall be followed. When a Special Operations LCO requires another LCO to be met, only the requirements of the LCO statement are required to be met regardless of that LCO's Applicability (i.e., should the requirements of this other LCO not be met, the ACTIONS of the Special Operations LCO apply, not the ACTIONS of the other LCO). However, there are instances where the Special Operations LCO ACTIONS may direct the other LCOs' ACTIONS be met. The

BASES

LCO 3.0.7 (continued)

Surveillances of the other LCO are not required to be met, unless specified in the Special Operations LCO. If conditions exist such that the Applicability of any other LCO is met, all the other LCO's requirements (ACTIONS and SRs) are required to be met concurrent with the requirements of the Special Operations LCO.

B 3.0 SURVEILLANCE REQUIREMENT (SR) APPLICABILITY

BASES

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

SR 3.0.1

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

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

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 Operations LCO are only applicable when the Special Operations LCO is used as an allowable exception to the requirements of a Specification.

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

BASES

SR 3.0.1 (continued)

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.

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. An example of this process is Control Rod Drive maintenance during refueling that requires scram testing at reactor steam dome pressure ≥ 6.55 MPaG (950 psig). However, if other appropriate testing is satisfactorily completed and the scram time testing of SR 3.1.4.3 is satisfied, the control rod can be considered OPERABLE. This allows startup to proceed to reach reactor steam dome pressure of 6.55 MPaG (950 psig) to perform other necessary 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).

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

BASES

SR 3.0.2 (continued)

25% extension of the interval specified in the Frequency does not apply. These exceptions are stated in the individual Specifications. The requirements of regulations take precedence over the TS. An example of where SR 3.0.2 does not apply is in the Primary Containment Leakage Rate Testing Program. This program establishes testing requirements and Frequencies in accordance with the requirements of regulations. The TS cannot in and of themselves extend a test interval specified in the regulations.

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

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

SR 3.0.3

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

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

SR 3.0.3 (continued)

The basis for this delay period includes consideration of unit conditions, adequate planning, availability of personnel, the time required to perform the Surveillance, the safety significance of the delay in completing the required Surveillance, and the recognition that the most probable result of any particular Surveillance being performed is the verification of conformance with the requirements. When a Surveillance with a Frequency based not on time intervals, but upon specified unit conditions, operating situations, or requirements of regulations (e.g., prior to entering MODE 1 after each fuel loading, or in accordance with 10 CFR 50, Appendix J, as modified by approved exemptions, etc.) is discovered to not have been performed when specified, SR 3.0.3 allows for the full delay period of up to the specified Frequency to perform the Surveillance. However, since there is not a time interval specified, the missed Surveillance should be performed at the first reasonable opportunity.

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

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

BASES

SR 3.0.3 (continued)

depth and rigor of the evaluation should be commensurate with the importance of the component. Missed Surveillances for important components should be analyzed quantitatively. If the results of the risk evaluation determine the risk increase is significant, this evaluation should be used to determine the safest course of action. All missed Surveillances will be placed in the licensee's Corrective Action Program.

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

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

SR 3.0.4

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

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

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

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, division, component, device, or variable is inoperable or outside its specified limits, the associated SR(s)

BASES

SR 3.0.4 (continued)

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

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

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

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.1 SHUTDOWN MARGIN (SDM)

BASES

BACKGROUND

SDM requirements are specified to ensure:

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; and

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

These requirements are satisfied by the control rods, as described in GDC 26 (Ref. 1), which can compensate for the reactivity effects of the fuel and water temperature changes experienced during all operating conditions.

APPLICABLE SAFETY ANALYSES

SDM is an explicit assumption in several of the evaluations in Chapter 15, Safety Analyses. SDM is assumed as an initial condition for the control rod removal error during refueling accident (Ref. 2). The analysis of these reactivity insertion events assumes the refueling interlocks are OPERABLE when the reactor is in the refueling mode of operation. These interlocks prevent the withdrawal of more than one control rod, or control rod pair, from the core during refueling. (Special consideration and requirements for multiple control rod withdrawal during refueling are covered in Special Operations LCO 3.10.6, "Multiple Control Rod Withdrawal - Refueling.") The analysis assumes this condition is acceptable since the core will be shutdown with the highest worth control rod or rod pair withdrawn, if adequate SDM has been demonstrated.

Prevention or mitigation of reactivity insertion events is necessary to limit energy deposition in the fuel to prevent significant fuel damage, which could result in undue release of radioactivity (see Bases for LCO 3.1.6, "Rod Pattern Control"). Adequate SDM ensures inadvertent criticalities will not cause significant fuel damage.

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

BASES

LCO	The specified SDM limit accounts for the uncertainty in the demonstration of SDM by testing. Separate SDM limits are provided for testing where the highest worth control rod or rod pair is determined analytically or by measurement. This is due to the reduced uncertainty in the SDM test when the highest worth control rod or rod pair is determined by measurement. When SDM is demonstrated by calculations not associated with a test (e.g., to confirm SDM during the fuel loading sequence), additional margin must be added to the specified SDM limit to account for uncertainties in the calculation. To assure adequate SDM, a design margin is included to account for uncertainties in the design calculations (Ref. 3).
APPLICABILITY	In MODES 1 and 2, SDM must be provided because subcriticality with the highest worth control rod or rod pair withdrawn is assumed in the analysis. In MODES 3, 4, and 5, SDM is required to ensure the reactor will be held subcritical with margin for a single withdrawn control rod or rod pair. SDM is required in MODE 6 to prevent an inadvertent criticality during the withdrawal of a single control rod from a core cell containing one or more fuel assemblies or of a control rod pair from loaded core cells during scram time testing.
ACTIONS	<u>A.1</u> With SDM not within the limits of the LCO in MODE 1 or 2, SDM must be restored within 6 hours. Failure to meet the specified SDM may be caused by a control rod that cannot be inserted. The 6-hour Completion Time is acceptable considering that the reactor can still be shut down assuming no additional failures of control rods to insert, and the low probability of an event occurring during this interval. <u>B.1</u> If the SDM cannot be restored, the reactor must be in MODE 3 within 12 hours to prevent the potential for further reductions in available SDM (e.g., additional stuck control rods). The allowed Completion Time of 12 hours is reasonable, based on operating experience, to reach MODE 3 from full power in an orderly manner and without challenging plant systems.

BASES

ACTIONS (continued)

C.1

With SDM not within limits in MODE 3 or 4, the operator must immediately initiate action to fully insert all insertable control rods. This action results in the least reactive condition for the core.

D.1 and D.2

With SDM not within limits in MODE 5, the operator must immediately initiate action to fully insert all insertable control rods. Action must continue until all insertable control rods are fully inserted. This action results in the least reactive condition for the core. Action must also be initiated immediately to establish reactor building refueling and pool area HVAC subsystem (REPAVS) and contaminated area HVAC subsystem (CONAVS) area isolation boundary. This can be accomplished by isolating the REPAVS and CONAVS dampers or verifying the automatic capability of the respective exhaust high radiation function.

E.1, E.2, and E.3

With SDM not within limits in MODE 6, the operator must immediately suspend CORE ALTERATIONS that could reduce SDM (e.g., insertion of fuel in the core or withdrawal of control rods). Suspension of these activities shall not preclude completion of movement of a component to a safe condition. Inserting control rods or removing fuel from the core will reduce the total reactivity and are therefore excluded from the suspended actions.

Action must also be immediately initiated to fully insert all insertable control rods in core cells containing one or more fuel assemblies. Actions must continue until all insertable control rods in core cells containing one or more fuel assemblies have been fully inserted. Control rods in core cells containing no fuel assemblies do not affect the reactivity of the core and therefore do not have to be inserted.

Action must also be initiated immediately to establish reactor building REPAVS and CONAVS area isolation boundary. This can be accomplished by isolating the REPAVS and CONAVS dampers or verifying the automatic capability of the respective exhaust high radiation function.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.1.1.1

Adequate SDM is verified to ensure the reactor can be made subcritical from any initial operating condition. Adequate SDM must be demonstrated by testing before or during the first startup after fuel movement, shuffling within the reactor pressure vessel, or control rod replacement. Control rod replacement refers to the decoupling and removal of a control rod from a core location, and subsequent replacement with a new control rod or a control rod from another core location. Since core reactivity will vary during the cycle as a function of fuel depletion and poison burnup, the beginning of cycle (BOC) test must also account for changes in core reactivity during the cycle. Therefore, to obtain the SDM, the initial measured value of core reactivity must be increased by an adder, R, which is the difference between the calculated value of maximum core reactivity during the operating cycle and the calculated BOC core reactivity. If the value of R is negative (that is, BOC is the most reactive point in the cycle), no correction to the BOC measured value is required (Ref. 4). For the SDM demonstrations that rely solely on calculation of the highest worth control rod, additional margin (0.10% $\Delta k/k$) must be added to the SDM limit to account for uncertainties in the calculation.

The SDM may be demonstrated during an in-sequence control rod withdrawal, in which the highest worth control rod pair is analytically determined, or during local criticals, where the highest worth control rod pair is determined by testing. Local critical tests require the withdrawal of out of sequence control rods. This testing could therefore require bypassing of the Rod Pattern Control System to allow the out of sequence withdrawal, so additional requirements must be met (see LCO 3.10.7, "Control Rod Testing - Operating").

The Frequency of 4 hours after reaching criticality is allowed to provide a reasonable time to perform the required calculations and appropriate verification.

During MODE 6, adequate SDM is also required to ensure the reactor does not reach criticality during control rod withdrawals. An evaluation of each in-vessel fuel movement during fuel loading (including shuffling fuel within the core) shall be performed to ensure adequate SDM is maintained during refueling. This ensures the intermediate loading patterns are bounded by the safety analyses for the final core loading pattern. For example, bounding analyses, which demonstrate adequate SDM for the most reactive configurations during the refueling, may be performed to demonstrate acceptability of the entire fuel movement

BASES

SURVEILLANCE REQUIREMENTS (continued)

sequence. For these SDM demonstrations, which rely solely on calculation, additional margin must be added to the specified SDM limit to account for uncertainties in the calculation. Spiral off-load or reload sequences inherently satisfy the SR provided the fuel assemblies are reloaded in the same configuration analyzed for the new cycle. Removing fuel from the core will always result in an increase in SDM.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 26.
2. Section 15.3.7.
3. NEDC-33239P-A, GE14 for ESBWR Nuclear Design Report, Revision 5, October 2010.
4. Section 4.3.3.3.1.

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.2 Reactivity Anomalies

BASES

BACKGROUND

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

When the reactor core is critical or in normal power operation, a reactivity balance exists and the net reactivity is zero. A comparison of predicted and measured reactivity is convenient under such a balance since parameters are being maintained relatively stable under steady state power conditions. The positive reactivity inherent in the core design is balanced by the negative reactivity of the control components, thermal feedback, neutron leakage, and materials in the core that absorb neutrons, such as burnable absorbers, producing zero net reactivity.

In order to achieve the required fuel cycle energy output, the uranium enrichment in the new fuel loading and the fuel loaded in the previous cycles provide excess positive reactivity beyond that required to sustain steady state operation at the beginning of cycle (BOC). When the reactor is critical at RTP and operating moderator temperature, the excess positive reactivity is compensated by burnable absorbers (if any), control rods, and whatever neutron poisons (mainly xenon and samarium) are present in the fuel.

The predicted core reactivity, as represented by k-effective (k_{eff}), is calculated by a 3D core simulator code as a function of cycle exposure. This calculation is performed for projected operating states and conditions throughout the cycle. The monitored k_{eff} is calculated by the core

BASES

BACKGROUND (continued)

monitoring system for actual plant conditions and is then compared to the predicted value for the cycle exposure.

APPLICABLE SAFETY ANALYSES

Accurate prediction of core reactivity is either an explicit or implicit assumption in many of the safety analyses in Chapter 15 (Ref. 2). In particular, SDM and reactivity transients, such as control rod withdrawal error events are very sensitive to accurate prediction of core reactivity. These analyses rely on computer codes that have been qualified against available test data, operating plant data, and analytical benchmarks. Monitoring reactivity anomaly provides additional assurance that the nuclear methods provide an accurate representation of the core reactivity.

The comparison between measured and predicted initial core reactivity provides a normalization for the calculational models used to predict core reactivity. If the measured and predicted k_{eff} for identical core conditions at BOC do not reasonably agree, then the assumptions used in the reload cycle design analysis or the calculation models used to predict k_{eff} may not be accurate. If reasonable agreement between measured and predicted core reactivity exists at BOC, then the prediction may be normalized to the measured value. Thereafter, any significant deviations in the measured k_{eff} from the predicted k_{eff} that develop during fuel depletion may be an indication that the assumptions of the design basis transient and accident analyses are no longer valid, or that an unexpected change in core conditions has occurred.

Reactivity Anomalies satisfy Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

The reactivity anomaly limit is established to ensure plant operation is maintained within the assumptions of the safety analyses. Large differences between monitored and predicted core reactivity may indicate that the assumptions of the design basis transient and accident analyses are no longer valid, or that the uncertainties in the Nuclear Design Methodology are larger than expected. A limit on the difference between the monitored core k_{eff} and the predicted core k_{eff} of ± 1% $\Delta k/k$ has been established based on engineering judgment. A > 1% deviation in reactivity from that predicted is larger than expected for normal operation and should therefore be evaluated.

BASES

APPLICABILITY

In MODE 1, most of the control rods are withdrawn and steady-state operation is typically achieved. Under these conditions, the comparison between predicted and monitored core reactivity provides an effective measure of the reactivity anomaly. In MODE 2, control rods are typically being withdrawn during a startup. In MODES 3, 4 and 5, all control rods are fully inserted, and, therefore, the reactor is in the least reactive state where monitoring core reactivity is not necessary. In MODE 6, fuel loading results in a continually changing core reactivity. SDM requirements (LCO 3.1.1) ensure that fuel movements are performed within the bounds of the safety analyses, and a SDM demonstration is required during the first startup following operations that could have altered core reactivity (e.g., fuel movement, control rod replacement, control rod shuffling). The SDM test, required by LCO 3.1.1, provides a direct comparison of the predicted and monitored core reactivity at cold conditions, and, therefore, reactivity anomaly is not required during these conditions.

ACTIONS

A.1

Should an anomaly develop between measured and predicted core reactivity, the core reactivity difference must be restored within the limit to ensure continued operation is within the core design assumptions. Restoration to within the limit could be performed by an evaluation of the core design and safety analysis to determine the reason for the anomaly. This evaluation normally reviews the core conditions to determine their consistency with input to design calculations. Measured core and process parameters are also normally evaluated to determine that they are within the bounds of the safety analysis, and safety analysis calculational models may be reviewed to verify that they are adequate for representation of the core conditions. The required Completion Time of 72 hours is acceptable based on the low probability of a Design Basis Accident occurring during this interval and allows sufficient time to assess the physical condition of the reactor and to complete an evaluation of the core design and safety analysis.

B.1

The unit must be placed in a MODE in which the LCO does not apply if the core reactivity cannot be restored to within the 1% $\Delta k/k$ limit. This is done by placing the unit in at least MODE 3 within 12 hours. The allowed

BASES

ACTIONS (continued)

Completion Time of 12 hours is reasonable, based on operating experience, to reach MODE 3 from full power in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.1.2.1

Verifying the reactivity difference between the monitored and predicted core k_{eff} is within the limits of the LCO provides added assurance that plant operation is maintained within the assumptions of the design basis transient and accident analyses. The core monitoring system calculates the core k_{eff} for the reactor conditions obtained from plant instrumentation. A comparison of the monitored core k_{eff} to the predicted core k_{eff} at the same cycle exposure is used to calculate the reactivity difference. The comparison is required when the core reactivity has potentially changed by a significant amount. This may occur following a refueling in which new fuel assemblies are loaded, fuel assemblies are shuffled within the core, or control rods are replaced or shuffled. Control rod replacement refers to the decoupling and removal of a control rod from a core location, and subsequent replacement with a new control rod or a control rod from another core location. Also, core reactivity changes during the cycle. The 24 hour interval after reaching equilibrium conditions following a startup was established based on the need for equilibrium xenon concentrations in the core such that an accurate comparison between the monitored and predicted core k_{eff} values can be made. For the purposes of this SR, the reactor is assumed to be at equilibrium conditions when steady state operations (no control rod movement) at ≥ 75% RTP have been obtained. The 1000 MWD/T Frequency was developed considering the relatively slow change in core reactivity with exposure and operating experience related to variations in core reactivity. This comparison requires the core to be operating at power levels which minimize the uncertainties and measurement errors, in order to obtain meaningful results. Therefore, the comparison is only done when in MODE 1.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 26, GDC 28, and GDC 29.
2. Chapter 15.

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.3 Control Rod OPERABILITY

BASES

BACKGROUND

Control rods are components of the Control Rod Drive (CRD) System, which is the primary Reactivity Control System for the reactor. In conjunction with the Reactor Protection System (RPS), the CRD System provides the means for the reliable control of reactivity changes to ensure that under conditions of normal operation, including anticipated operational occurrences, specified acceptable fuel design limits are not exceeded. In addition, the control rods provide the capability to hold the reactor core subcritical under all conditions and to limit the potential amount and rate of reactivity increase caused by a malfunction in the CRD System. The CRD System is designed to satisfy the requirements of GDC 26, GDC 27, GDC 28, and GDC 29 (Ref. 1).

The CRD System consists of 269 fine motion control rod drive (FMCRD) mechanisms and 135 hydraulic control unit (HCU) assemblies. The FMCRD is an electro-hydraulic actuated mechanism that provides normal positioning of the control rods using an electric motor, and scram insertion of the control rods using hydraulic power. The hydraulic power for scram is provided by high pressure water stored in the individual HCU accumulators, each of which supplies sufficient volume to scram two FMCRDs. Normal control rod positioning is performed using a ball-nut and rotating ballscrew arrangement driven by an electric motor. A hollow piston, which is coupled at the upper end to the control rod, rests on the ball-nut. The ball-nut inserts the hollow piston and connected control rod into the core or withdraws them depending on the direction of rotation of the motor. An electromechanical brake mechanism engages the motor drive shaft when the motor is deenergized to prevent inadvertent withdrawal of the control rod, but does not restrict scram insertion.

This Specification along with LCO 3.1.4, "Control Rod Scram Times," and LCO 3.1.5, "Control Rod Scram Accumulators," ensures that the performance of the control rods in the event of a Design Basis Accident (DBA) or transient meets the assumptions used in the safety analyses of References 2, 3, 4, 5 and 6.

BASES

APPLICABLE SAFETY ANALYSES

The analytical methods and assumptions used in the evaluations involving control rods are presented in References 2, 3, 4, 5, and 6. The control rods provide the primary means for rapid reactivity control (reactor scram), for maintaining the reactor subcritical, and for limiting the potential effects of reactivity insertion events caused by malfunctions in the CRD System.

The capability to insert the control rods ensures that the assumptions for scram reactivity in the design basis transient and accident analyses are not violated. Since the SDM ensures the reactor will be subcritical with the highest worth control rod or control rod pair withdrawn (assumed single failure of an hydraulic control unit (HCU)), the failure of an additional control rod or control rod pair to insert, if required, could invalidate the demonstrated SDM and potentially limit the ability of the CRD System to hold the reactor subcritical. Therefore, the requirement that all control rods be OPERABLE ensures the CRD System can perform its intended function.

The control rods also protect the fuel from damage that could result in release of radioactivity. The limits protected are the Fuel Cladding Integrity Safety Limit (SL) (see Bases for SL 2.1.1, "Reactor Core SLs," and LCO 3.2.2, "MINIMUM CRITICAL POWER RATIO (MCPR)"), the 1% cladding plastic strain fuel design limit (see Bases for LCO 3.2.1, "LINEAR HEAT GENERATION RATE (LHGR)"), and the fuel damage limit (see Bases for LCO 3.1.6, "Rod Pattern Control") during reactivity insertion events.

The negative reactivity insertion (scram) provided by the CRD System provides the analytical basis for determination of plant thermal limits and provides protection against fuel damage limits during a Rod Withdrawal Error (RWE) event. Bases for LCO 3.1.4, LCO 3.1.5, and LCO 3.1.6 discuss in more detail how the SLs are protected by the CRD System.

Control Rod OPERABILITY satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

OPERABILITY of an individual control rod is based on a combination of factors, primarily the scram insertion times, the control rod coupling integrity, and the ability to determine the control rod position. Accumulator OPERABILITY is addressed by LCO 3.1.5. The associated scram accumulator status for a control rod only affects the scram insertion times and therefore an inoperable accumulator does not immediately require declaring a control rod inoperable.

BASES

LCO (continued)

Although not all control rods are required to be OPERABLE to satisfy the intended reactivity control requirements, strict control over the number and distribution of inoperable control rods is required to satisfy the assumptions of the design basis transient and accident analyses.

APPLICABILITY

In MODES 1 and 2, the control rods are assumed to function during a DBA or transient and are therefore required to be OPERABLE in these MODES. In MODES 3, 4, and 5, control rods are not able to be withdrawn since the reactor mode switch is in shutdown and a control rod block is applied. This provides adequate requirements for control rod OPERABILITY during these conditions. Control rod requirements in MODE 6 are located in LCO 3.9.5, "Control Rod OPERABILITY - Refueling."

ACTIONS

The ACTIONS Table is modified by two Notes. The first Note allows separate Condition entry for each control rod. This is acceptable since the Required Actions for each Condition provides appropriate compensatory actions for each inoperable control rod. Complying with the Required Actions may allow for continued operation, and subsequent inoperable control rods governed by subsequent Condition entry and application of associated Required Actions. The second Note requires entry into applicable Conditions and Required Actions of LCO 3.7.6, "Selected Control Rod Run-In (SCRRI) and Select Rod Insert (SRI) Functions," when inoperable control rods result in inoperability of the SRI function. This Note is necessary to ensure that the ACTIONS for an inoperable SRI are taken if the control rod inoperability affects the OPERABILITY of the SRI function. Otherwise, pursuant to LCO 3.0.6, these ACTIONS would not be entered even when the LCO 3.7.6 is not met. Therefore, Note 2 is added to require the proper actions are taken.

COL 16.0-1-A 3.1.3-1

[A.1, A.2, A.3, and A.4][A.1, A.2, and A.3]

A control rod is stuck if it will not insert by either FMCRD motor torque or hydraulic scram pressure. A control rod is not made inoperable by a failure of the FMCRD motor if the rod is capable of hydraulic scram. With a fully inserted control rod stuck, no actions are required as long as the control rod remains fully inserted. The Required Actions are modified by a Note that allows a stuck control rod to be bypassed in the Rod Control and Information System (RC&IS) to allow continued operation.

BASES

ACTIONS (continued)

SR 3.3.2.1.9 provides additional requirements when control rods are bypassed in the RC&IS to ensure compliance with the RWE analysis.

COL 16.0-1-A 3.1.3-1

[With one withdrawn control rod stuck, the local scram reactivity rate assumptions may not be met if the stuck control rod separation criteria are not met. Therefore, a verification that the separation criteria are met must be performed immediately. The separation criteria are not met if: a) the stuck control rod occupies a location adjacent to two "slow" control rods, b) the stuck control rod occupies a location adjacent to one "slow" control rod, and the one "slow" control rod is also adjacent to another "slow" control rod, or c) if the stuck control rod occupies a location adjacent to one "slow" control rod when there is another pair of "slow" control rods adjacent to one another. The description of "slow" control rods is provided in LCO 3.1.4, "Control Rod Scram Times." In addition, t][T]he associated control rod drive must be disarmed and isolated within 2 hours. The allowed Completion Time of 2 hours is acceptable, considering the reactor can still be shut down, assuming no additional control rods fail to insert, and provides a reasonable amount of time to perform the Required Action in an orderly manner.

The motor drive may be disarmed by bypassing the rod in the RC&IS or disconnecting its power supply. Isolating the control rod from scram prevents damage to the CRD and surrounding fuel assemblies should a scram occur. The control rod can be isolated from scram by isolating it from its associated HCU. Two CRDs sharing an HCU can be individually isolated from scram.

Monitoring of the insertion capability of withdrawn control rods must be performed within 24 hours from discovery of Condition A concurrent with THERMAL POWER greater than the low power setpoint (LPSP) of the RC&IS. SR 3.1.3.2 and SR 3.1.3.3 perform periodic tests of the control rod insertion capability of withdrawn control rods. Testing within 24 hours ensures a generic problem does not exist. This Completion Time allows for an exception to the normal "time zero" for beginning the allowed

COL 16.0-1-A 3.1.3-1

outage time "clock." The Required Action A.[3][2] Completion Time only begins upon discovery of Condition A concurrent with THERMAL POWER greater than the actual LPSP of the RC&IS, since the notch insertions may not be compatible with the requirements of rod pattern control (LCO 3.1.6) and the RC&IS (LCO 3.3.2.1, "Control Rod Block Instrumentation") when below the actual LPSP. The allowed Completion Time of 24 hours from discovery of Condition A, concurrent with

BASES

ACTIONS (continued)

THERMAL POWER greater than the LPSP of the RC&IS, provides a reasonable time to test the control rods, considering the potential for a need to reduce power to perform the tests.

To allow continued operation with a withdrawn control rod stuck, an evaluation of adequate SDM is also required within 72 hours. Should a design basis transient or accident require a shutdown, to preserve the single failure criterion, an additional control rod would have to be assumed to fail to insert when required. Therefore, the original SDM demonstration may not be valid. The SDM must therefore be evaluated (by measurement or analysis) with the stuck control rod withdrawn and the highest worth control rod or control rod pair assumed to be fully withdrawn.

The allowed Completion Time of 72 hours to verify SDM is adequate considering that with a single control rod stuck in the withdrawn position, the remaining OPERABLE control rods are capable of providing the required scram and shutdown reactivity. Failure to reach MODE 5 is only likely if an additional control rod adjacent to the stuck control rod also fails to insert during a required scram. Even with the postulated additional single failure of an adjacent control rod to insert, sufficient reactivity control remains to reach and maintain MODE 3 or 4 conditions. In addition, Required Action A.[3][2] performs a movement test on each remaining withdrawn control rod to ensure that no additional control rods are stuck. Therefore, the 72 hour Completion Time to perform the SDM verification in Required Action A.[4][3] is acceptable.

COL 16.0-1-A
3.1.3-1

B.1

With two or more withdrawn control rods stuck, the plant must be brought to MODE 3 within 12 hours. The occurrence of more than one control rod stuck at a withdrawn position increases the probability that the reactor cannot be shut down if required. Insertion of all insertable control rods eliminates the possibility of an additional failure of a control rod to insert. The allowed Completion Time of 12 hours is reasonable, based on operating experience, to reach MODE 3 from full power in an orderly manner and without challenging plant systems.

C.1 and C.2

With one or more control rods inoperable for reasons other than being stuck in the withdrawn position, operation may continue, provided the

BASES

ACTIONS (continued)

control rods are fully inserted within 3 hours and disarmed (however, they do not need to be isolated from scram). Inserting a control rod ensures the shutdown and scram capabilities are not adversely affected. The control rod is disarmed to prevent inadvertent withdrawal during subsequent operations. The control rods can be disarmed by bypassing the rod in the RC&IS or disconnecting its power supply. Required Action C.1 is modified by a Note that allows control rods to be bypassed in the RC&IS if required to allow insertion of the inoperable control rods and continued operation. SR 3.3.2.1.9 provides additional requirements when the control rods are bypassed to ensure compliance with the RWE analysis.

The allowed Completion Times are reasonable considering the small number of allowed inoperable control rods and provides time to insert and disarm the control rods in an orderly manner and without challenging plant systems.

D.1 and D.2

During reactor startup at less than 50% control rod density, the Ganged Withdrawal Sequence Restrictions (GWSR) analysis requires inserted control rods not in compliance with GWSR to be separated by at least two OPERABLE control rods in all directions including the diagonal (Ref. 2). Out-of-sequence control rods may increase the potential reactivity worth of a control rod, or gang of control rods, during a RWE and therefore the distribution of inoperable control rods must be controlled. Therefore, if two or more inoperable control rods are not in compliance with GWSR and not within separation limits as specified in the COLR, actions must be taken to restore compliance with GWSR or restore the control rods to OPERABLE status. A Note has been added to the Condition to clarify that the Condition is not applicable when > 10% RTP since the GWSR is not required to be followed under these conditions, as described in the Bases for LCO 3.1.6.

E.1

If any Required Action and associated Completion Time of Condition A, C, D, or E are not met or nine or more inoperable control rods exist, 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 12 hours. This ensures all insertable control rods are inserted and places the reactor in a condition that does not require the active function (i.e., scram)

BASES

ACTIONS (continued)

of the control rods. The number of control rods permitted to be inoperable when operating above 10% RTP could be more than the value specified, but the occurrence of a large number of inoperable control rods could be indicative of a generic problem, and investigation and resolution of the potential problem should be undertaken. The allowed Completion Time of 12 hours is reasonable, based on operating experience, to reach MODE 3 in an orderly manner from full power without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.1.3.1

Determining the position of each control rod is required to ensure adequate information on control rod position is available to the operator for determining CRD OPERABILITY and controlling rod patterns. Control rod position may be determined by the use of OPERABLE position indicators, or by the use of other appropriate methods. The 24-hour Frequency of this SR is based on operating experience related to expected changes in control rod position and the availability of control rod position indication in the control room.

SR 3.1.3.2 and SR 3.1.3.3

Control rod insertion capability is demonstrated by inserting each partially or fully withdrawn control rod two notches (i.e., 4 steps) and observing that the control rod moves. The control rod may then be returned to its original position. This ensures the control rod is not stuck and is free to insert on a scram signal. These surveillances are not required when below the actual LPSP of the RC&IS since the step insertions may not be compatible with the requirements of the Ganged Withdrawal Sequence Restrictions (LCO 3.1.6) and the RC&IS (LCO 3.3.2.1). The 7 day Frequency of SR 3.1.3.2 is based on experience related to changes in CRD performance and the ease of performing step testing for fully withdrawn control rods. Partially withdrawn control rods are tested with a 31 day Frequency based on the potential power reduction required to allow the control rod movement and considering the large testing sample of SR 3.1.3.2. Furthermore, the 31 day Frequency takes into account operating experience related to changes in CRD performance. At any time, if a control rod is immovable, a determination of that control rod's trippability (OPERABILITY) must be made and appropriate action taken.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.1.3.4

COL 16.0-1-A 3.1.3-2

Verifying the scram time for each control rod [to [60]% rod insertion position is less than or equal to [ ] seconds][ ]provides reasonable assurance that the control rod will insert when required during a DBA or transient, thereby completing its shutdown function. This SR is performed in conjunction with the control rod scram time testing of SR 3.1.4.1, SR 3.1.4.2, SR 3.1.4.3, and SR 3.1.4.4. The CHANNEL FUNCTIONAL TEST in LCO 3.3.1.1, "Reactor Protection System (RPS) Instrumentation," and the LOGIC SYSTEM FUNCTIONAL TEST in LCO 3.3.1.2, "Reactor Protection System (RPS) Actuation," overlaps this Surveillance to provide complete testing of the assumed safety function. The associated Frequencies are acceptable, considering the more frequent testing performed to demonstrate other aspects of control rod OPERABILITY and operating experience, which shows scram times do not significantly change over an operating cycle.

SR 3.1.3.5

Coupling verification is performed to confirm the integrity of the coupling between the control rod and the hollow piston and to ensure the control rod will perform its intended function when necessary. The Surveillance requires verifying that a control rod does not go to the withdrawn overtravel position when it is fully withdrawn. The overtravel position feature provides a positive check on the coupling integrity, since only an uncoupled hollow piston can reach the overtravel position. The verification is required to be performed prior to declaring the control rod OPERABLE after work on the control rod or CRD System that could affect the coupling.

This Frequency is acceptable because of the mechanical integrity of the bayonet coupling design of the FMCRDs. The bayonet coupling can only be engaged/disengaged by performing a 45° rotation of the FMCRD mechanism relative to the control rod. This is normally performed by rotating the FMCRD mechanism 45° from below the vessel with the control rod kept from rotating by the orificed fuel support that has been installed from above. Once the coupling is engaged and the FMCRD middle flange is bolted into place, the 45° rotation required for uncoupling cannot be accomplished unless the associated orificed fuel support is removed (which would allow for the control rod to be rotated from above) or the FMCRD middle flange is unbolted (which would allow for rotation of the FMCRD mechanism from below). Therefore, after FMCRD

BASES

SURVEILLANCE REQUIREMENTS (continued)

maintenance in which the FMCRD is uncoupled and then recoupled or after the orificed fuel support has been moved, it is required to perform a coupling verification. Thereafter, it is not necessary to check the coupling integrity again until the FMCRD maintenance work has resulted in uncoupling and recoupling, or the orificed fuel support has been moved.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 26, GDC 27, GDC 28, and GDC 29.
2. NEDE-33243P-A, ESBWR Control Rod Nuclear Design, Revision 2, September 2010.
3. Section 4.3.3.
4. Section 4.6.1.
5. Section 5.2.2.
6. Chapter 15.

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.4 Control Rod Scram Times

BASES

BACKGROUND

The scram function of the Control Rod Drive (CRD) System controls reactivity changes during abnormal operational transients to ensure that specified acceptable fuel design limits are not exceeded (Ref. 1). The control rods are scrammed by positive means, using hydraulic pressure exerted on the CRD piston.

A single hydraulic control unit (HCU) powers the scram action of one or two fine motion control rod drives (FMCRDs). When a scram signal is initiated, control air is vented from the scram valve in each hydraulic control unit (HCU), allowing it to open by spring action. High pressure nitrogen then raises the piston within the HCU accumulator and forces the displaced water through the scram piping to the connected FMCRDs. Inside each FMCRD, the high pressure water lifts the hollow piston off the ball-nut and drives the control rod into the core. A buffer assembly stops the hollow piston at the end of its stroke. Departure from the ball-nut releases spring-loaded latches in the hollow piston that engage slots in the guide tube. These latches support the control rod in the inserted position. The control rod cannot be withdrawn until the ball-nut is driven up and engaged with the hollow piston. Stationary fingers on the ball-nut then cam the latches out of the slots and hold them in the retracted position. A scram action is complete when every FMCRD has reached their fully inserted position.

APPLICABLE SAFETY ANALYSES

The analytical methods and assumptions used in evaluating the control rod scram function are presented in References 2, 3, 4, 5, and 6. The design basis transient and accident analyses assume that all of the control rods scram at a specified insertion rate. The resulting negative scram reactivity forms the basis for the determination of plant thermal limits (e.g., the MCPR). [Other distributions of scram times (e.g., several control rods scramming slower than the average time, with several control rods scramming faster than the average time) can also provide sufficient scram reactivity.][ ]Surveillance of each individual control rod's scram time ensures that the scram reactivity assumed in the design basis transient and accident analyses can be met.

COL 16.0-1-A 3.1.4-1

The scram function of the CRD System protects the Fuel Cladding Integrity Safety Limit (SL) (see Bases for SL 2.1.1, "Reactor Core SLs," and LCO 3.2.2, "MINIMUM CRITICAL POWER RATIO (MCPR)"), and the

BASES

APPLICABLE SAFETY ANALYSES (continued)

1% cladding plastic strain fuel design limit (see Bases for LCO 3.2.1, "LINEAR HEAT GENERATION RATE (LHGR)"), which ensure that no fuel damage will occur if these limits are not exceeded. For reactor pressures above 7.340 MPaG (1065 psig), the scram function is designed to insert negative reactivity at a rate fast enough to prevent the Fuel Cladding Integrity SL being exceeded during the analyzed limiting power transient. For reactor pressures below 7.340 MPaG (1065 psig) the scram function is assumed to function during the Rod Withdrawal Error (RWE) event (Ref. 6) and, therefore, also provides protection against violating fuel damage limits during reactivity insertion accidents (see Bases for LCO 3.1.6, "Rod Pattern Control"). For the reactor vessel overpressure protection analysis, the scram function, along with the Safety Relief Valves, ensures that the peak vessel pressure is maintained within the applicable ASME Code limits.

Control Rod Scram Times satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

The scram time limits specified in Table 3.1.4-1 (in the accompanying LCO) are required to ensure that the scram reactivity assumed in the design basis transient and accident analysis is met. [To account for single failure and "slow" scramming control rods, the scram time limits specified in Table 3.1.4-1 are faster than those assumed in the design basis analysis. The scram time limits have a margin to allow up to [8] of the control rods to have scram times that exceed the specified limits (i.e., "slow" control rods) assuming a single stuck control rod (as allowed by LCO 3.1.3, "Control Rod OPERABILITY") and an additional control rod or control rod pair failing to scram per the single failure criterion.][ ]The scram time limits are specified as a function of reactor steam dome pressure to account for the pressure dependence of the scram times. The scram time limits are specified relative to percent insertion. The scram time limits are specified relative to measurements based on reed switch positions, which provide the control rod position indication. The reed switch closes ("pickup") when the hollow piston passes a specific location and then opens ("dropout") as the hollow piston tube travels upward. Verification of the specified scram times in Table 3.1.4-1 is accomplished through measurement of the "dropout" times.

COL 16.0-1-A 3.1.4-1

[To ensure that local scram reactivity rates are maintained within acceptable limits, no more than two of the allowed "slow" control rods may occupy adjacent locations.

BASES

LCO (continued)

COL 16.0-1-A 3.1.4-1

Table 3.1.4-1 is modified by two Notes, which state control rods with scram times not within the limits of the Table are considered "slow" and that control rods with scram times > [ ] seconds to [60]% insertion are considered inoperable as required by SR 3.1.3.4, and are not considered slow.][ ]

COL 16.0-1-A 3.1.4-1

This LCO applies only to OPERABLE control rods since inoperable control rods will be inserted and disarmed (LCO 3.1.3).[Slow scramming control rods may be conservatively declared inoperable and not accounted for as "slow" control rods.][ ]

APPLICABILITY

In MODES 1 and 2, a scram is assumed to function during transients and accidents analyzed for these plant conditions. These events are assumed to occur during startup and power operation; therefore, the scram function of the control rods is required during these MODES. In MODES 3, 4, and 5, the control rods are not able to be withdrawn since the reactor mode switch is in shutdown and a control rod block is applied. This provides adequate requirements for control rod scram capability during these conditions. Scram requirements in MODE 6 are contained in LCO 3.9.5, "Control Rod OPERABILITY - Refueling".

ACTIONS

A.1

COL 16.0-1-A 3.1.4-1

When the requirements of this LCO are not met, the rate of negative reactivity insertion during a scram may not be within the assumptions of the safety analyses. [Therefore, 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 12 hours. The allowed Completion Time of 12 hours is reasonable, based on operating experience, to reach MODE 3 from full power in an orderly manner and without challenging plant systems.][Therefore, the affected control rod must be declared inoperable, and the Actions of LCO 3.1.3 entered.]

BASES

SURVEILLANCE REQUIREMENTS

All four SRs of this LCO are modified by a Note stating that during a single control rod or control rod pair scram time Surveillance, the CRD pumps shall be isolated from the associated scram accumulator. With the CRD pump isolated (i.e., charging valve closed) the influence of the CRD pump head does not affect the single control rod or control rod pair scram times. During a full core scram, the CRD pump head would be seen by all control rods and would have a negligible effect on the scram insertion times.

SR 3.1.4.1

The scram reactivity used in design basis transient and accident analyses is based on assumed control rod scram time. Measurement of the scram times with reactor steam dome pressure ≥ 6.55 MPaG (950 psig) demonstrates acceptable scram times for the transients analyzed in References 4 and 5.

Scram insertion times increase with increasing reactor pressure because of the competing effects of reactor steam dome pressure and stored accumulator energy. Demonstration of adequate scram times at reactor steam dome pressure ≥ 6.55 MPaG (950 psig) helps to ensure that the scram times will be within the specified limits at higher pressures. Limits are specified as a function of reactor pressure to account for the sensitivity of the scram insertion times with pressure and to allow a range of pressures over which scram time testing can be performed. To ensure that scram time testing is performed within a reasonable time following a refueling or after a shutdown greater than 120 days or longer, control rods are required to be tested before exceeding 40% RTP following the shutdown. This Frequency is acceptable considering the additional surveillances performed for control rod OPERABILITY, the frequent verification of adequate accumulator pressure, and the required testing of control rods affected by work on control rods or the CRD System.

SR 3.1.4.2

Additional testing of a sample of control rods is required to verify the continued performance of the scram function during the cycle. A representative sample contains at least 10% of the control rods, the sample remains representative if no more than 7.5% of the control rods in the sample tested are determined to be ["slow."][inoperable.] If more than 7.5% of the sample is declared to be ["slow" per the criteria in][inoperable based on the acceptance criteria in] Table 3.1.4-1, additional control rods are tested until this 7.5% criterion (e.g., 7.5% of the sample size) is

COL 16.0-1-A 3.1.4-1

BASES

SURVEILLANCE REQUIREMENTS (continued)

satisfied, or until the total number of ["slow"][inoperable] control rods (throughout the core, from all Surveillances) [exceeds the LCO limit][results in entering Action D of LCO 3.1.3]. For planned testing, the control rods selected for the sample should be different for each test. Data from inadvertent scrams should be used whenever possible to avoid unnecessary testing at power, even if the control rods with data were previously tested in a sample. The 200 day Frequency is based on operating experience that has shown that control rod scram times do not significantly change over an operating cycle. This Frequency is also reasonable based on the additional Surveillances done on the control rod drives at more frequent intervals in accordance with LCO 3.1.3 and LCO 3.1.5, "Control Rod Scram Accumulators."

SR 3.1.4.3

When work is performed on a control rod or the CRD System that could affect the scram insertion time, testing must be done to demonstrate that each affected control rod retains adequate scram performance over the range of applicable reactor pressures from zero to the maximum permissible pressure. The scram testing must be performed before declaring the control rod OPERABLE. The required scram time testing must demonstrate that the affected control rod is still within acceptable limits. The limits for reactor pressures < 7.340 MPaG (1065 psig) are established based on a high probability of meeting the acceptance criteria at reactor pressures ≥ 7.340 MPaG (1065 psig). Limits for reactor pressures ≥ 7.340 MPaG (1065 psig) are found in Table 3.1.4-1. [If testing demonstrates the affected control rod does not meet these limits, but is within the limit of Table 3.1.4-1, Note 2, the control rod can be declared OPERABLE and "slow."][ ]

COL 16.0-1-A 3.1.4-1

Specific examples of work that could affect the scram times include (but are not limited to) the following: removal of any CRD for maintenance or modification, replacement of a control rod, and maintenance or modification of a scram solenoid pilot valve, scram valve, accumulator isolation valve, or check valves in the piping required for scram.

The Frequency of once prior to declaring the affected control rod OPERABLE is acceptable because of the capability to test the control rods over a range of operating conditions and the more frequent surveillances on other aspects of control rod OPERABILITY.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.1.4.4

After fuel movement has occurred within the affected cell or after work on a control rod or the CRD System has occurred that can affect scram time, the scram insertion time must be confirmed. Testing must be done to demonstrate each affected control rod is still within the limits of Table 3.1.4-1 with the reactor steam dome pressure ≥ 6.55 MPaG (950 psig). Where work has been performed at high reactor pressure, the requirements of SR 3.1.4.3 and SR 3.1.4.4 will be satisfied with one test. For a control rod affected by work performed while shut down, however, a zero pressure and a high pressure test may be required. This testing ensures that the control rod scram performance is acceptable for operating reactor pressure conditions prior to withdrawing the control rod for continued operation. Alternatively, a test during hydrostatic pressure testing could also satisfy both criteria. When fuel movement within the reactor pressure vessel occurs, only those control rods associated with the core cells affected by the fuel movement are required to be scram time tested. During a routine refueling outage, it is expected that all control rods will be affected.

The Frequency of once prior to exceeding 40% RTP is acceptable because of the capability to test the control rods at the different conditions and the more frequent surveillances on other aspects of control rod OPERABILITY.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 10.
2. Section 4.2.4.
3. Section 4.3.3.
4. Section 4.6.1.
5. Section 5.2.2.
6. Chapter 15.

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.5 Control Rod Scram Accumulators

BASES

BACKGROUND	The control rod scram accumulators are part of the Control Rod Drive (CRD) System and are provided to ensure that the control rods scram under varying reactor conditions. The control rod scram accumulators store sufficient energy to fully insert a single or pair of control rods associated with a specific hydraulic control unit (HCU) at any reactor vessel pressure. The accumulator is a hydraulic cylinder with a free-floating piston. The piston separates the water used to scram the control rods from the nitrogen, which provides the required energy. The scram accumulators are necessary to scram the control rods within the required insertion times of LCO 3.1.4, "Control Rod Scram Times."
APPLICABLE SAFETY ANALYSES	The analytical methods and assumptions used in evaluating the control rod scram function are presented in References 1, 2, 3, and 4. The design basis transient and accident analyses assume that all of the control rods scram at a specified insertion rate. OPERABILITY of each individual control rod scram accumulator, along with LCO 3.1.3, "Control Rod OPERABILITY," and LCO 3.1.4, ensures that the scram reactivity assumed in the design basis transient and accident analyses can be met. The existence of an inoperable accumulator may invalidate prior scram time measurements for the associated control rods. The scram function of the CRD System, and, therefore, the OPERABILITY of the accumulators, protects the Fuel Cladding Integrity Safety Limit (see Bases for LCO 3.2.2 "MINIMUM CRITICAL POWER RATIO (MCPR)") and the 1% cladding plastic strain fuel design limit (see Bases for LCO 3.2.1, "LINEAR HEAT GENERATION RATE (LHGR)"), which ensure that no fuel damage will occur if these limits are not exceeded (see Bases for LCO 3.1.4). Also, the scram function at low reactor vessel pressure (i.e., startup conditions) provides protection against violating fuel design limits during reactivity insertion accidents (see Bases for LCO 3.1.6, "Rod Pattern Control"). Control Rod Scram Accumulators satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO	The OPERABILITY of the control rod scram accumulators is required to ensure that adequate scram insertion capability exists when needed over the entire range of reactor pressures. The OPERABILITY of the scram accumulators is based on maintaining adequate accumulator pressure.
APPLICABILITY	In MODES 1 and 2, the scram function is required for mitigation of DBAs and transients and, therefore, the scram accumulators must be OPERABLE to support the scram function. In MODES 3, 4, and 5, control rods are not able to be withdrawn since the reactor mode switch is in shutdown and a control rod block is applied. This provides adequate requirements for control rod scram accumulator OPERABILITY under these conditions. Requirements for scram accumulators in MODE 6 are contained in LCO 3.9.5, "Control Rod OPERABILITY - Refueling."

ACTIONS

The ACTIONS Table is modified by a Note indicating that a separate Condition entry is allowed for each control rod scram accumulator. This is acceptable since the Required Actions for each Condition provide appropriate compensatory action for each inoperable control rod scram accumulator. Complying with the Required Actions may allow for continued operation and subsequent inoperable accumulators governed by subsequent Condition entry and application of associated Required Actions.

A.1

With one control rod scram accumulator inoperable, the scram function could become severely degraded because the accumulator is the primary source of scram force for the associated control rod or rod pair at all reactor pressures. In this event, the associated control rod or rod pair is declared inoperable and LCO 3.1.3 entered. This would result in requiring the affected control rod or rod pair to be fully inserted and disarmed, thereby satisfying its intended function in accordance with ACTIONS of LCO 3.1.3. The allowed Completion Time of 8 hours is considered reasonable, based on the large number of control rods available to provide the scram function. Additionally, an automatic reactor scram function is provided on sensed low pressure in the scram

BASES

ACTIONS (continued)

accumulator charging water header (see LCO 3.3.1.1, "Reactor Protection System (RPS) Instrumentation"). This anticipatory reactor trip protects against the possibility of significant pressure degradation (and thus reduced scram force) concurrently in multiple control rod scram accumulators due to a transient in the CRD hydraulic system.

B.1

With two or more control rod scram accumulators inoperable, the scram function could become severely degraded because the accumulators are the primary source of scram force for the control rods at all reactor pressures. In this event, the associated control rods are declared inoperable and LCO 3.1.3 entered. This would result in requiring the affected control rods to be fully inserted and disarmed, thereby satisfying its intended function in accordance with ACTIONS of LCO 3.1.3.

The allowed Completion Time of 1 hour is considered reasonable based on engineering judgment considering the low probability of a DBA or transient occurring while the affected accumulators are inoperable.

C.1

The reactor mode switch must be immediately placed in the shutdown position if any Required Action and associated Completion Time cannot be met. This ensures that all insertable control rods are inserted and that the reactor is in a condition that does not require the active function (i.e., scram) of the control rods. This Required Action is modified by a Note stating that the Required Action is not applicable if all control rods associated with the inoperable scram accumulators are fully inserted, since the function of the control rods has been performed.

SURVEILLANCE REQUIREMENTS

SR 3.1.5.1

SR 3.1.5.1 requires that the accumulator pressure be checked every 7 days to ensure that adequate accumulator pressure exists to provide sufficient scram force. The primary indicator of accumulator OPERABILITY is the accumulator pressure. A minimum accumulator pressure is specified, below which the capability of the accumulator to perform its intended function becomes degraded and the accumulator is considered inoperable. The minimum accumulator pressure of

COL 16.0-1-A 3.1.5-1

[12.76 MPaG (1850 psig) is well below the expected pressure of 14.82 MPaG (2150 psig) (Ref. 2)].

BASES

SURVEILLANCE REQUIREMENTS (continued)

Declaring the accumulator inoperable when the minimum pressure is not maintained ensures that significant degradation in scram times does not occur. The 7 day Frequency has been shown to be acceptable through operating experience and takes into account other indications available in the control room.

REFERENCES

1. Section 4.3.3.
2. Section 4.6.1.
3. Section 5.2.2.
4. Chapter 15.

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.6 Rod Pattern Control

BASES

BACKGROUND	Control rod patterns during startup conditions are controlled by the operator and the rod worth minimizer (RWM), (LCO 3.3.2.1, "Control Rod Block Instrumentation"), so that only specified control rod sequences and relative positions are allowed over the operating range from all control rods inserted to 10% RTP. The sequences effectively limit the potential amount of reactivity addition that could occur during a control rod withdrawal, specifically the Rod Withdrawal Error (RWE) event.
APPLICABLE SAFETY ANALYSES	The analytical methods and assumptions used in evaluating the RWE are summarized in Reference 1. RWE analyses assume that the reactor operator follows prescribed withdrawal sequences. These sequences define the potential initial conditions for the RWE analysis. The RWM provides backup to operator control of the withdrawal sequences to ensure that the initial conditions of the RWE analysis are not violated. Control rod patterns analyzed in Reference 1 follow the Ganged Withdrawal Sequence Restrictions (GWSR). The GWSR is applicable from the condition of all control rods fully inserted to 10% RTP. For GWSR, the control rods are required to be moved in groups, with all OPERABLE control rods assigned to specific groups required not to exceed an allowable maximum position difference until all OPERABLE control rods of the group have reached a defined withdrawal position. The GWSR are defined to minimize the maximum incremental control rod worths without being overly restrictive during normal plant operation. Prevention or mitigation of positive reactivity insertion events is necessary to limit energy deposition in the fuel to prevent significant fuel damage which could result in undue release of radioactivity. Analysis of the GWSR (Ref. 1) has demonstrated that the 712 J/g (170 cal/g) limit for evaluating the radiological consequences of an RWE will not be violated. The analysis also evaluated the effect of fully inserted inoperable control rods not in compliance with the sequence to allow a limited number (i.e., eight) and distribution of fully inserted inoperable control rods. Rod Pattern Control satisfies the requirements of Criterion 3 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO	Compliance with the prescribed control rod sequences minimizes the potential consequences of a RWE by limiting the initial conditions to those consistent with the GWSR. This LCO only applies to OPERABLE control rods. For inoperable control rods required to be inserted, separate requirements are specified in LCO 3.1.3, "Control Rod OPERABILITY," consistent with the allowances for inoperable control rods in the GWSR.
APPLICABILITY	Compliance with GWSR is required in MODES 1 and 2 when THERMAL POWER is ≤ 10% of RTP. When THERMAL POWER is > 10% of RTP, there is no possible control rod configuration that results in a control rod worth that could exceed the 712 J/g (170 cal/g) limit for evaluating the radiological consequences of an RWE. In MODES 3, 4, 5, and 6, since the reactor is shutdown and only a total of one control rod or control rod pair can be withdrawn from core cells containing fuel assemblies, adequate SDM ensures the reactor will remain subcritical.

ACTIONS

A.1 and A.2

With one or more OPERABLE control rods not in compliance with the prescribed control rod sequence, actions may be taken to either correct the control rod pattern or declare the associated control rods inoperable within 8 hours. Noncompliance with the prescribed sequence may be the result of failed resolvers, or a power reduction to ≤ 10% RTP before establishing the correct control rod pattern (i.e., a pattern that complies with the GWSR). The number of OPERABLE control rods not in compliance with the prescribed sequence is limited to eight to prevent the operator from attempting to correct a control rod pattern that significantly deviates from the prescribed sequence. When the control rod pattern is not in compliance with the prescribed sequence, all control rod movement should be stopped except for moves needed to correct the control rod pattern, or scram if warranted.

Required Action A.1 is modified by a Note which allows control rods to be bypassed in Rod Control & Information System (RC&IS) to allow the affected control rods to be returned to their correct position. This ensures that the control rods will be moved to the correct position. A control rod not in compliance with the prescribed sequence is not considered inoperable except as required by Required Action A.2. OPERABILITY of control rods is determined by compliance with LCO 3.1.3, LCO 3.1.4, "Control Rod Scram Times," and LCO 3.1.5, "Control Rod Scram Accumulators." The allowed Completion Time of 8 hours is reasonable, considering the restrictions on the number of allowed out-of-sequence

BASES

ACTIONS (continued)

control rods and the low probability of a RWE occurring during the time the control rods are out of sequence.

B.1 and B.2

If nine or more OPERABLE control rods are out of sequence the control rod pattern significantly deviates from the prescribed sequence. Control rod withdrawal should be suspended immediately to prevent the potential for further deviation from the prescribed sequence. Control rod insertion to correct control rods withdrawn beyond their allowed position is allowed since, in general, insertion of control rods has less impact on control rod worths than withdrawals. Required Action B.1 is modified by a Note that allows the affected control rods to be bypassed in RC&IS in accordance with SR 3.3.2.1.9 to allow insertion only. With nine or more OPERABLE control rods not in compliance with GWSR, the reactor mode switch must be placed in the shutdown position within one hour. With the reactor mode switch in shutdown, the reactor is shut down and as such does not meet the applicability requirements of this LCO. The allowed Completion Time of 1 hour is a reasonable time to allow insertion of control rods to restore compliance, and is appropriate relative to the low probability of a RWE occurring with the control rods out of sequence.

SURVEILLANCE REQUIREMENTS

SR 3.1.6.1

Verification that the control rod pattern is in compliance with the GWSR at a 24 hour Frequency ensures that the assumptions of the RWE analyses are met. The 24 hour Frequency of this Surveillance was developed considering that the primary check of the control rod pattern compliance with the GWSR is performed by the RWM (LCO 3.3.2.1). The RWM provides control rod blocks to enforce the required control rod sequence and is required to be OPERABLE when operating ≤ 10% RTP.

REFERENCES

1. Section 15.3.8.

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.7 Standby Liquid Control (SLC) System

BASES

BACKGROUND

The SLC System is designed to provide both manual and automatically initiated capability for bringing the reactor, at any time in a fuel cycle, from full power and minimum control rod inventory (which is at the peak of the xenon transient), to a subcritical condition with the reactor in the most reactive xenon-free state without taking credit for control rod movement. The SLC System satisfies portions of the requirements of 10 CFR 50.62 (Ref. 1) on anticipated transient without scram (ATWS). The automatic initiation signals applicable to ATWS mitigation are addressed in the Availability Control Manual.

The SLC System is also credited in the loss of coolant accident (LOCA) to provide makeup water to the Reactor Pressure Vessel (RPV). The emergency core cooling system (ECCS) and the SLC are designed to flood the core during a LOCA to provide required core cooling. By providing core cooling following a LOCA, the ECCS, including SLC, in conjunction with the containment, limit the release of radioactive materials to the environment following a LOCA. The injection of sodium pentaborate is also credited for buffering the pH in containment pools following a LOCA.

The SLC System contains two identical and separate trains. Each train provides 50% of the required SLC injection capacity required for ATWS. Each train also provides 50% of the required SLC injection capacity assumed to be available for a LOCA. Each train consists of a nitrogen-pressurized accumulator containing sodium pentaborate solution (SPBS). Each train is connected to the RPV through piping that includes two, normally open, SLC accumulator isolation valves in series and two injection squib valves in parallel. The SPBS is injected into the RPV by firing squib valves.

Each SLC injection line is connected to an RPV supply header. Each header includes spargers with a total of eight nozzles. Each nozzle penetrates the shroud and is provided with two holes that discharge the SPBS into the core. This arrangement, together with a high nozzle injection velocity, assures proper distribution of the SPBS within the core bypass region. Boron in sodium pentaborate acts as a neutron poison reducing and halting the fission process. The SLC System is passive and requires no high pressure pump or external standby AC power for SPBS injection. Power for the safety functions of the SLCS is derived from the

BASES

BACKGROUND (continued)

safety-related 120 VAC electrical systems. Adequate functioning of the SLC System requires only one of the two injection valves open in each SLC train.

Each SLC train includes two injection squib valves, which are arranged in parallel. Actuation of either injection squib valve provides the required flow path for injection of the associated SLC train. Each of the injection squib valves are equipped with two safety-related squib initiators that are actuated by the safety-related Safety System Logic and Control (SSLC) described in the Bases for LCO 3.3.5.1, "Emergency Core Cooling System (ECCS) Instrumentation," and LCO 3.3.5.2, "Emergency Core Cooling System (ECCS) Actuation."

Each SLC train includes two, normally open, accumulator isolation valves, which are arranged in series, and close on a low accumulator level signal from any two of the four SLC accumulator level sensors associated with each accumulator. Closure of either accumulator isolation valve is sufficient to prevent the injection of nitrogen from the accumulator into the RPV. The normally open accumulator isolation valves receive an open signal to support the ECCS injection function.

Power to each of the safety-related squib initiators on each SLC injection squib valve is supplied from a different division of the DC and Uninterruptible AC Electrical Power Distribution. As such, at least one safety-related initiator in each SLC injection squib valve will be associated with DC and Uninterruptible AC Electrical Power Distribution Divisions required by LCO 3.8.6, "Distribution Systems - Operating."

SLC is designed to ensure that no single active component failure will cause inadvertent initiation or prevent initiation and successful operation.

APPLICABLE SAFETY ANALYSES

The ECCS function of the SLC System is automatically initiated as described in the Bases for LCO 3.3.5.1. During a LOCA, SLC provides makeup water to the RPV to ensure the core is cooled (Ref. 2). The injection of sodium pentaborate is also credited for buffering the pH in containment pools following a LOCA (Ref. 3).

The SLC System injects borated water into the reactor core to compensate for all of the various reactivity effects that could occur during plant operation. To meet this objective, a quantity of isotopically enriched

APPLICABLE SAFETY ANALYSES (continued)

SPBS is injected, which produces the equivalent shutdown capability as concentration of 760 ppm of natural, non-enriched SPBS in the reactor core at 20°C (68°F). The volume and concentration limits are calculated such that the required concentration is achieved accounting for dilution in the RPV with the reactor water level conservatively taken at the elevation of the bottom edge of the main steamlines. This result is then increased by a factor of 1.25 to provide a 25% general margin to discount potential nonuniformities of the mixing process within the reactor (Ref. 4). That result is then increased by a factor of 1.15 to provide a further margin of 15% to discount potential dilution by the Reactor Water Cleanup/Shutdown Cooling (RWCU/SDC) System when activated in the shutdown cooling mode.

The SLC System satisfies Criteria 3 and 4 of 10 CFR 50.36(c)(2)(ii).

LCO

The OPERABILITY of the SLC System provides backup capability for reactivity control independent of normal reactivity control provisions provided by the control rods. In addition, the SLC System provides makeup water to the RPV to mitigate the consequences of a LOCA. For ATWS requirements, the OPERABILITY of the SLC System is based on the conditions of the borated solution in each accumulator and the availability of a pressurized accumulator and a flow path from each accumulator to the RPV, including the OPERABILITY of the instrumentation and valves. For a LOCA, the volume of water in both SLC accumulators is necessary for makeup and core cooling.

Two SLC trains are required to be OPERABLE, each containing two OPERABLE injection squib valves and two OPERABLE accumulator isolation valves in the open position and associated piping, valves, and instruments and controls to ensure an OPERABLE flow path.

OPERABILITY of each injection squib valve requires OPERABILITY of one safety-related initiator associated with DC and Uninterruptible AC Electrical Power Distribution Divisions required by LCO 3.8.6. OPERABILITY of each accumulator isolation valve requires OPERABILITY of safety-related closing initiators and safety-related opening initiators associated with DC and Uninterruptible AC Electrical Power Distribution Divisions required by LCO 3.8.6.

BASES

APPLICABILITY

In MODES 1 and 2, the SLC System is needed for its reactor shutdown capability. Reactor shutdown capability is not required in MODES 3, 4 and 5 because the reactor mode switch is in shutdown and control rods cannot be withdrawn because a control rod block is applied. When a control rod block is not applied, LCO 3.10.3, “Control Rod Withdrawal – Hot / Stable Shutdown,” and LCO 3.10.4, “Control Rod Withdrawal – Cold Shutdown,” in conjunction with LCO 3.1.1, "SHUTDOWN MARGIN," provide adequate controls to ensure the reactor remains subcritical.

In MODES 1, 2, 3, and 4, the ECCS function of SLC System is required to provide additional inventory for RPV water makeup and core cooling.

ACTIONS

[A.1

If the concentration of sodium pentaborate in solution in one or more accumulators is not within limits, the concentration must be restored to within limits in 72 hours. For ATWS mitigation the plant design also includes, alternate rod insertion (ARI), fine motion control rod drive run-in, and a feedwater runback features as described in Reference 5. These additional features provide ATWS mitigation capability when the concentration of sodium pentaborate in solution is not within limits. Because of the low probability of an ATWS event, the additional ATWS mitigation features, and the fact that SLC System capability still exists for vessel injection under these conditions, the allowed Completion Time of 72 hours is acceptable and provides adequate time to restore concentration to within limits.]

COL 16.0-1-A 3.1.7-1

[B].1

With one injection squib valve flow path in one or more trains inoperable, the squib valve flow path(s) must be restored to OPERABLE status within 7 days. In this condition, the remaining OPERABLE squib valve flow paths are adequate to perform the shutdown function. However, the overall reliability is reduced because a single failure in the remaining OPERABLE squib valve flow paths could result in reduced SLC System capability. The 7 day Completion Time is based on engineering judgment considering the availability of one OPERABLE flow path in each train that is capable of performing the intended SLC System function and the low probability of a Design Basis Accident (DBA) or transient occurring during this period.

BASES

ACTIONS (continued)

COL 16.0-1-A 3.1.7-1

[C].1

With one accumulator isolation valve inoperable for closing in one or more trains, the accumulator isolation valve(s) must be restored to OPERABLE status within 7 days. In this condition, the remaining OPERABLE accumulator isolation valve is capable of performing the required safety function. However, the overall reliability is reduced because a single failure in the remaining OPERABLE isolation valve could result in injection of nitrogen into the RPV. The 7 day Completion Time is based on engineering judgment considering the availability of one OPERABLE flow path in each train that is capable of performing the intended SLC System function and the low probability of a DBA or transient occurring during this period.

[D].1 and [D].2

COL 16.0-1-A 3.1.7-1

If one or more SLC trains are inoperable for reasons other than Condition A[, B, or C] (e.g., one or both accumulator isolation valve in the closed position), or if any Required Action and associated Completion Time of Condition A[, B, or C] 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 MODE 3 within 12 hours and MODE 5 within 36 hours. The allowed Completion Times are reasonable, based on plant design, to reach MODE 5 from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.1.7.1, SR 3.1.7.2, and SR 3.1.7.3

SR 3.1.7.1 through SR 3.1.7.3 are 24 hour Surveillances verifying certain characteristics of the SLC System (e.g., the volume of sodium pentaborate solution in the accumulator, temperature of the room with piping and valves containing boron solution, and nitrogen volume and pressure in each accumulator), thereby ensuring the SLC System OPERABILITY without disturbing normal plant operation. These Surveillances ensure the proper SPBS volume and temperature and

BASES

SURVEILLANCE REQUIREMENTS (continued)

accumulator nitrogen volume and pressure are maintained. Maintaining a minimum specified SPBS temperature is important in ensuring that the boron remains in solution and does not precipitate in the accumulators or in the injection piping. Maintaining a minimum accumulator nitrogen volume and pressure will ensure the full injection of solution inventory at rated reactor pressure. The 24 hour Frequency of these SRs was based on operating experience that has shown that there are relatively slow variations room temperature and alarms that monitor volume and pressure.

SR 3.1.7.4

This SR requires verification every 31 days of the continuity of one safety-related initiator associated with DC and Uninterruptible AC Electrical Power Distribution Divisions required by LCO 3.8.6 for each injection squib valve.

The 31 day Frequency is acceptable because either of the two injection squib valves in each train is capable of initiating SLC injection. Additionally, an alarm will provide prompt notification of loss of circuit continuity for the required initiators in each SLC injection valve.

This SR is modified by a Note that continuity is not required to be met for one required initiator intermittently disabled under administrative controls. This allows the continuity monitor to be tested and allows surveillance and maintenance with the assurance that the valve will not be opened inadvertently. The operation of the disable/test switch in either division does not disable the SLC system because the parallel injection squib valve will still be opened by the initiator in another other division.

SR 3.1.7.5

SR 3.1.7.5 verifies each valve in the system is in its correct position but does not apply to the squib valves. Verifying the correct alignment for manual, power-operated, and automatic valves in the SLC System flow path provides assurance that the proper flow paths will exist for system operation. This Surveillance 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 verification of valve alignment does not apply to valves which cannot be inadvertently misaligned, such as check valves. This SR does not require any testing or valve manipulation; rather, it involves verification that those valves

BASES

SURVEILLANCE REQUIREMENTS (continued)

capable of being mispositioned are in the correct positions. The 31 day Frequency for SR 3.1.7.5 is appropriate because the valves are operated under procedural control and it was chosen to provide added assurance that the valves are in the correct positions.

This SR is modified by a Note allowing an SLC flow path to be isolated intermittently under administrative controls. These controls consist of stationing a dedicated operator, who is in continuous communication with the control room, at the controls of the valve to open the valve when a valid actuation signal is indicated.

SR 3.1.7.6

This Surveillance requires an examination of the sodium pentaborate solution by using chemical analysis to ensure the proper concentration of boron exists in the accumulator. SR 3.1.7.6 must be performed any time boron or water is added to the accumulator solution to establish that the boron solution concentration is within the specified limits. This Surveillance must be performed anytime the temperature is restored to within the limits of Figure 3.1.7-1, to ensure no significant boron precipitation occurred. The 31 day Frequency of this Surveillance is appropriate because the boron solution is not expected to change concentration between surveillances.

SR 3.1.7.7

The SLC trains are required to actuate both automatically and manually to perform their design function. This Surveillance test verifies that, with a required system initiation signal (actual or simulated), the SLC operates as designed when initiated either by an actual or simulated initiation signal, causing proper actuation of all the required components, including isolation of the SLC accumulator when accumulator level is low. The LOGIC SYSTEM FUNCTIONAL TEST performed in LCO 3.3.5.2 overlaps this Surveillance to provide complete testing of the assumed SLC function.

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 an unplanned transient if the Surveillance were performed with the reactor at power. Operating experience has shown that these components usually pass the SR when performed at the 24 month Frequency, which is based on the refueling cycle. Therefore, the

BASES

SURVEILLANCE REQUIREMENTS (continued)

Frequency was concluded to be acceptable from a reliability standpoint.

This SR is modified by a Note that excludes valve actuation. This is acceptable because SLC valves are subject to the Inservice Test Program.

SR 3.1.7.8

This SR requires a CHANNEL CALIBRATION of the accumulator level instrumentation channels that actuate SLC accumulator isolation on low level. CHANNEL CALIBRATION is a complete check of the instrument loop and the sensor. This test verifies that the channel responds to the measured parameters within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to the required nominal trip setpoint within the "as-left tolerance" to account for instrument drifts between successive calibrations consistent with the methods and assumptions required by the Setpoint Control Program. The Frequency is based upon the assumption of a 24-month calibration interval in the determination of the magnitude of equipment drift in the setpoint analysis.

SR 3.1.7.9

This Surveillance ensures that there is a functioning flow path for the boron solution from the accumulator to the RPV. The Surveillance may be performed in overlapping steps, provided the entire flow path is verified within the specified Frequency. The flow path may be verified by flow tests using demineralized water to prevent injecting boron into the RPV, or a combination of flushing, visual inspection, or boroscopic inspection.

This SR is accompanied by a Note that excludes squib valve actuation as a requirement for this SR to be met. This is acceptable because squib valves are flanged, allowing access to both sides of the valves for verification that the flow path is free of obstructions. The squib valves are tested under the ASME OM Code and are included in the Inservice Testing Program (Ref. 6).

Each SLC train includes two parallel flow paths, each controlled by an injection squib valve. The Frequency, 24 months on a STAGGERED TEST BASIS for each flow path, ensures that the flow path tested every 24 months is alternated so that each flow path is tested every 96 months.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The 24 month Frequency is necessary because of the need to perform this Surveillance during a plant outage. The 24 month Frequency is acceptable because of the low probability that the piping will be blocked due to precipitation of the boron from solution. The saturation temperature of the solution is less than 15.5°C (60°F) (Ref. 4) and requirements in SR 3.1.7.2 conservatively ensure that the SPBS remains above saturation temperature. Additionally, the SLC mixing pump and sample connection may be used to verify flow through the outlet of the accumulator.

SR 3.1.7.10

Enriched sodium pentaborate solution is made by mixing granular, enriched sodium pentaborate with water. Isotopic tests on the granular sodium pentaborate to verify the actual B-10 enrichment must be performed prior to addition to the SLC accumulator to ensure that the proper B-10 atom percent is being used.

REFERENCES

1. 10 CFR 50.62.
2. Section 6.3.3.
3. Section 15.4.4.
4. Section 9.3.5.
5. Section 7.8.1.1.
6. Section 3.9.6.1.

B 3.2 POWER DISTRIBUTION LIMITS

B 3.2.1 LINEAR HEAT GENERATION RATE (LHGR)

BASES

BACKGROUND

The LHGR is a measure of the heat generation rate of a fuel rod in a fuel assembly at any axial location. Limits on the LHGR are specified to ensure that fuel design limits are not exceeded anywhere in the core during normal operation, including anticipated operational occurrences (AOOs). Exceeding the LHGR limit could potentially result in fuel damage and subsequent release of radioactive materials. Fuel design limits are specified to ensure that fuel system damage, fuel rod failure or inability to cool the fuel will not occur during the anticipated operating conditions identified in Reference 1.

APPLICABLE SAFETY ANALYSES

The analytical methods and assumptions used in evaluating the fuel system design are presented in References 1 and 2. The fuel assembly is designed to ensure (in conjunction with the core nuclear and thermal hydraulic design, plant equipment, instrumentation and protection system) that fuel damage will not result in the release of radioactive materials in excess of the guidelines of 10 CFR, Parts 20, 50, and 52.47(a)(2)(iv). The mechanisms that could cause fuel damage during operational transients and that are considered in fuel evaluations are:

a. Rupture of the fuel rod cladding caused by strain from the relative expansion of the UO_2 pellet; and

b. Severe overheating of the fuel rod cladding caused by inadequate cooling.

A value of 1% plastic strain of the fuel cladding has been defined as the limit below which fuel damage caused by overstraining of the fuel cladding is not expected to occur (Ref. 1). The Fuel Cladding Integrity Safety Limit ensures that fuel damage caused by severe overheating of the fuel cladding is avoided.

Fuel design evaluations have been performed and demonstrate that the 1% fuel cladding plastic strain design limit is not exceeded during continuous operation with LHGRs up to the operating limit specified in the COLR. The analysis also includes allowances for short-term transient operation above the operating limit to account for AOOs, plus an allowance for densification power spiking.

BASES

APPLICABLE SAFETY ANALYSES (continued)

The LHGR operating limit is power and feedwater temperature dependent. Therefore, the LHGR operating limits specified in the COLR include power dependent limits and feedwater temperature dependent limits.

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

LCO

The LHGR is a basic assumption in the fuel design analysis. The fuel has been designed to operate at rated core power with sufficient design margin to the LHGR calculated to cause 1% fuel cladding plastic strain. The operating limit to accomplish this objective is specified in the COLR.

APPLICABILITY

The LHGR limits are derived from fuel design analysis that is limiting at high power level conditions. At core thermal power levels < 25% RTP, the reactor is operating with a substantial margin to the LHGR limits and, therefore, the Specification is only required when the reactor is operating at ≥ 25% RTP.

ACTIONS

A.1

If any LHGR exceeds its required limit, an assumption regarding an initial condition of the fuel design analysis is not met. Therefore, prompt action should be taken to restore the LHGR(s) to within its required limits such that the plant is operating within analyzed conditions. The 2 hour Completion Time is normally sufficient to restore the LHGR(s) to within its limits and is acceptable based on the low probability of a transient or Design Basis Accident (DBA) occurring simultaneously with the LHGR out of specification.

BASES

ACTIONS (continued)

B.1

If the LHGR cannot be restored to within its required limits within the associated Completion Time, the plant must be brought to a MODE or other specified condition in which the LCO does not apply. To achieve this status, THERMAL POWER must be reduced to < 25% RTP within 4 hours. The 4 hour Completion Time is reasonable, based on engineering judgment, to reduce THERMAL POWER to < 25% RTP in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.2.1.1

The LHGRs are required to be initially calculated within 12 hours after THERMAL POWER is ≥ 25% RTP and then every 24 hours thereafter. They are compared to the specified limits in the COLR to ensure that the reactor is operating within the assumptions of the safety analysis. The 24 hour Frequency is based on both engineering judgment and recognition of the slowness of changes in power distribution under normal conditions. The 12 hour allowance after THERMAL POWER reaches ≥ 25% RTP is acceptable given the large inherent margin to operating limits at low power levels.

REFERENCES

1. Section 15.2.
2. Chapter 4.

B 3.2 POWER DISTRIBUTION LIMITS

B 3.2.2 MINIMUM CRITICAL POWER RATIO (MCPR)

BASES

BACKGROUND	MCPR is a ratio of the fuel assembly power that would result in the onset of boiling transition to the actual fuel assembly power. The Fuel Cladding Integrity Safety Limit (FCISL) is established as greater than 99.9% of the fuel rods in the core would be expected to avoid boiling transition (refer to the Bases for SL 2.1.1.2). The operating limit MCPR is established to ensure that no fuel damage results during anticipated operational occurrences (AOOs). Although fuel damage does not necessarily occur if a fuel rod actually experiences boiling transition (Ref. 1), the critical power at which boiling transition is calculated to occur has been adopted as a fuel design criterion. The onset of transition boiling is a phenomenon that is readily detected during the testing of various fuel bundle designs. Based on these experimental data, correlations have been developed to predict critical bundle power (i.e., the bundle power level at the onset of transition boiling) for a given set of plant parameters (e.g., reactor vessel pressure, mass flux, and subcooling). Because plant operating conditions and bundle power levels are monitored and determined relatively easily, monitoring the MCPR is a convenient way of ensuring that fuel failures due to inadequate cooling do not occur.
APPLICABLE SAFETY ANALYSES	The analytical methods and assumptions used in evaluating the AOOs to establish the operating limit MCPR are presented in Chapter 4. To ensure that the FCISL is not exceeded during any transient event that occurs with moderate frequency, limiting transients have been analyzed to determine the critical power ratio (CPR) transient uncertainty. The types of transients evaluated are decrease in core coolant temperature, increase in reactor pressure, increase in reactor coolant inventory, decrease in reactor coolant inventory. The steady-state and CPR transient uncertainties and the uncertainties in monitoring and simulating the core operating state are incorporated by the statistical model (Ref. 2) to determine the required operating limit MCPR. The transient analyses assume that the feedwater control system is in automatic mode; therefore, if the feedwater control system is in manual mode, then the MCPR LCO is not met.

BASES

APPLICABLE SAFETY ANALYSES (continued)

The MCPR operating limits are power and feedwater temperature dependent. Therefore, the MCPR operating limits specified in the COLR include power dependent limits and feedwater temperature dependent limits.

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

LCO

The MCPR operating limits specified in the COLR are the result of fuel design and transient analyses.

APPLICABILITY

The MCPR operating limits are primarily derived from transient analyses that are assumed to occur at high power levels. Below 25% RTP, the moderator void fraction is very small. Surveillance of thermal limits below 25% RTP is unnecessary due to the large inherent margin that ensures that the FCISL is not exceeded even if a limiting transient occurs.

Studies of the variation of limiting transient behavior have been performed over the range of operational conditions. These studies encompass the range of key actual plant parameter values important to typically limiting transients. The results of these studies demonstrate that a margin is expected between performance and the MCPR requirements, and that margins increase as power is reduced to 25% RTP. Comparison of test data at low pressure and flow conditions to expected bundle operating conditions at less than 25% RTP has determined that the bundle powers would have to increase by multiples of three or more prior to reaching critical bundle powers. When in MODE 2, the Startup Range Neutron Monitor (SRNM) provides rapid scram initiation for any significant power increase transient, which effectively eliminates any MCPR compliance concern. Therefore, at THERMAL POWER levels < 25% RTP, the reactor is operating with substantial margin to the MCPR limits and this LCO is not required.

BASES

ACTIONS

A.1

If any MCPR is outside the required limits, an assumption regarding an initial condition of the design basis transient analyses may not be met. Therefore, prompt action should be taken to restore the MCPR(s) to within the required limits such that the plant will be operating within analyzed conditions. The 2 hour Completion Time is normally sufficient to restore the MCPR(s) to within its limits and is acceptable based on the low probability of a transient occurring simultaneously with the MCPR out of specification.

B.1

If the MCPR cannot be restored to within its required limits within the associated Completion Time, the plant must be brought to a MODE or other specified condition in which the LCO does not apply. To achieve this status, THERMAL POWER must be reduced to < 25% RTP within 4 hours. The 4 hour Completion Time is reasonable, based on engineering judgment, to reduce THERMAL POWER to < 25% RTP in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.2.2.1

The MCPRs are required to be initially calculated within 12 hours after THERMAL POWER is ≥ 25% RTP and then every 24 hours thereafter. They are compared to the specified limits in the COLR to ensure that the reactor is operating within the assumptions of the safety analysis. The 24 hour Frequency is based on both engineering judgment and recognition of the slowness of changes in power distribution under normal conditions. The 12 hour allowance after THERMAL POWER reaches ≥ 25% RTP is acceptable given the large inherent margin to operating limits at low power levels.

REFERENCES

1. NUREG-0562, "Fuel Rod Failure as a Consequence of Departure From Nucleate Boiling or Dryout," June 1979.

2. NEDC-33237P-A, GE14 for ESBWR - Critical Power Correlation, Uncertainty, and OLMCPR Development, Revision 5, September 2010.

B 3.3 INSTRUMENTATION

B 3.3.1.1 Reactor Protection System (RPS) Instrumentation

BASES

BACKGROUND

The RPS is designed to initiate a reactor scram when one or more monitored parameters exceed their specified limit, to preserve the integrity of the fuel cladding and the Reactor Coolant System (RCS), and minimize the energy that must be absorbed following a loss of coolant accident (LOCA). This can be accomplished either automatically or manually.

The protection and monitoring functions of the RPS have been designed to ensure safe operation of the reactor. This is achieved by specifying limiting safety system settings (LSSS) in terms of parameters directly monitored by the RPS, as well as LCOs on other reactor system parameters and equipment performance.

Technical Specifications are required by 10 CFR 50.36 to contain LSSS defined by the regulation as "...settings for automatic protective devices related to those variables having significant safety functions." Where LSSS is specified for a variable on which a Safety Limit (SL) has been placed, the setting must be chosen such that automatic protective action will correct the abnormal situation before a SL is exceeded. The Analytical Limit is the limit of the process variable at which a safety action is initiated, as established by the safety analysis, to ensure that a SL is not exceeded. Any automatic protection action that occurs on reaching the Analytical Limit therefore ensures that the SL is not exceeded. Where LSSS is specified for a variable having a significant safety function but which does not protect SLs, the setting must be chosen such that automatic protective actions will initiate consistent with the design basis. The Design Limit is the limit of the process variable at which a safety action is initiated to ensure that these automatic protective devices will perform their specified safety function.

The actual settings for automatic protective devices must be chosen to be more conservative than the Analytical / Design Limit to account for instrument loop uncertainties related to the setting at which the automatic protective action would actually occur. The methodology for determining the actual settings, and the required tolerances to maintain these settings conservative to the Analytical / Design Limits, including the requirements for determining that the channel is OPERABLE, are defined in the Setpoint Control Program (SCP), in accordance with Specification 5.5.11, “Setpoint Control Program (SCP)."

BASES

BACKGROUND (continued)

The Limiting Trip Setpoint (LTSP) is a predetermined setting for a protective device chosen to ensure automatic actuation prior to the process variable reaching the Analytical / Design Limit and thus ensuring that the SL would not be exceeded (i.e., for Analytical Limits), or that automatic protective actions occur consistent with the design basis (i.e., for Design Limits). As such, the LTSP accounts for process and primary element measurement errors, and uncertainties in setting the device (e.g., calibration), uncertainties in how the device might actually perform (e.g., accuracy), changes in the point of action of the device over time (e.g., drift during surveillance intervals), and any other factors that may influence its actual performance (e.g., harsh accident environments). In this manner, the LTSP ensures that SLs are not exceeded and that automatic protective devices will perform their specified safety function. As such, the LTSP meets the definition of an LSSS. The nominal trip setpoint to which the setpoint is reset after calibration is the $NTSP_F$, which is more conservative than the LTSP and has margin to assure that the Allowable Value is not exceeded during calibration.

Technical Specifications contain values related to the OPERABILITY of equipment required for safe operation of the facility. OPERABLE is defined in Technical Specifications as "...being capable of performing its safety function(s)." For automatic protective devices, the required safety function is to ensure that a SL is not exceeded and that automatic protective actions will initiate consistent with the design basis. Therefore, the LTSP is the LSSS as defined by 10 CFR 50.36. However, use of the LTSP to define OPERABILITY in Technical Specifications would be an overly restrictive requirement if it were applied as an OPERABILITY limit for the "as-found" value of a protective device setting during a Surveillance.

However, there is also some point beyond which the device would have not been able to perform its function due, for example, to greater than expected drift. This value is specified in the SCP, as required by Specification 5.5.11, in order to define OPERABILITY of the devices and is designated as the Allowable Value which is the least conservative value of the as-found setpoint that a channel can have during CHANNEL CALIBRATION. The LTSP, $NTSP_F$, Allowable Value, "as-found" tolerance, and "as-left" tolerance, and the methodology for calculating the "as-left" and "as-found" tolerances will be maintained in the SCP, as required by Specification 5.5.11.

BASES

BACKGROUND (continued)

The Allowable Value is the least conservative value that the setpoint of the channel can have when tested such that a channel is OPERABLE if the setpoint is found conservative with respect to the Allowable Value during the CHANNEL CALIBRATION. Note that, although a channel is OPERABLE under these circumstances, the setpoint must be left adjusted to a value within the established "as-left" tolerance of the $NTSP_F$ and confirmed to be operating within the statistical allowances of the uncertainty terms assigned in the setpoint calculation. As such, the Allowable Value differs from the $NTSP_F$ by an amount equal to or greater than the "as-found" tolerance value. In this manner, the actual setting of the device will ensure that a SL is not exceeded or that automatic protective actions will initiate consistent with the design basis at any given point of time as long as the device has not drifted beyond that expected during the surveillance interval. If the actual setting of the device is found to be non-conservative with respect to the Allowable Value the device would be considered inoperable from a Technical Specification perspective. This requires corrective action including those actions required by 10 CFR 50.36 when automatic protective devices do not function as required.

The RPS, as shown in Reference 1, is divided into four redundant divisions of sensor (instrument) channels, trip logics and trip actuators, and two divisions of manual scram controls and scram logic circuitry. The sensor channels, divisions of trip logic, divisions of trip actuators, and associated portions of the divisions of scram logic circuitry together constitute the RPS automatic scram and backup scram initiation logic. The divisions of manual scram controls and associated portions of the divisions of scram logic circuitry together constitute the RPS manual scram and backup scram initiation logic. The automatic and manual scram initiation logics are independent of each other and use diverse methods and equipment to initiate a reactor scram.

Instrument (Sensor) Channels

Equipment within a sensor channel consists of sensors (i.e., transducers or switches), Digital Trip Module (DTM) and multiplexers. The sensors within each channel detect abnormal operating conditions and send analog (or discrete) output either directly to the RPS cabinets or to Remote Multiplexer Units (RMUs) within the associated division. The RMU within each division performs analog-to-digital conversion on analog signals and sends the digital or digitized analog output values of the monitored variables to the DTM for trip determinations within the

BACKGROUND (continued)

associated RPS Instrument (sensor) channel in the same division. The DTM in each sensor channel compares individual monitored variable values with trip setpoint values and for each variable sends a separate trip/no trip output signal to the functional Trip Logic Units (TLUs) in the four divisions of trip logic. Equipment within a single division is powered from the safety-related power source of the same division. OPERABILITY requirements for instrument channels are addressed in LCO 3.3.1.1.

Divisions of Trip Logic

Equipment within an RPS division of trip logic consists of TLUs, manual switches, bypass units (BPUs) and Output Logic Units (OLUs). The TLUs perform the automatic scram initiation logic, checking for two-out-of-four coincidence of trip conditions in any set of instrument channel signals coming from the four divisions of DTMs or from isolated digital inputs from the four divisions of the Neutron Monitoring System (NMS), and outputting a trip signal if any one of the two-out-of-four coincidence checks is satisfied. The automatic scram initiation logic for any trip is based on the reactor operating mode status and channel trip conditions and bypass conditions. Each TLU, besides receiving isolated digital input trip signals from the four divisions of DTMs, also receives digital input signals from the BPU and other control interfaces in the same division.

The various manual switches provide the operator with the means to enforce interlocks within RPS trip logic for special operation, maintenance, testing, and system reset. The BPUs perform bypass and interlock logic for the division of sensors bypass and the division of logic bypass. Each BPU sends its divisional sensor bypass signal to the TLU of the same division and an isolated divisional sensor bypass signal to the TLUs of the other three divisions. Each BPU sends its divisional logic bypass signal to the OLU of the same division and an isolated divisional logic bypass signal to the OLUs of the other three divisions. The OLUs perform division trip, seal-in, reset and trip test functions. Each OLU receives bypass inputs from the BPU and trip inputs from the TLU of the same division. Each OLU provides trip outputs to the trip actuators.

BASES

BACKGROUND (continued)

Equipment within a division of trip logic is powered from the same division of safety-related power source. However, different pieces of equipment are powered from separate low voltage dc power supplies in the same division. OPERABILITY requirements for the Divisions of Trip Logic are addressed in LCO 3.3.1.2, "Reactor Protections System (RPS) Actuation," with the exception of the digital trip function, which is addressed in LCO 3.3.1.1.

Divisions of Trip Actuators

Equipment within a division of trip actuators includes load drivers for automatic primary scram and output contactors for the initiation of backup scram. The RPS includes two physically separate and electrically independent divisions of trip actuators that receive inputs from the four divisions of the OLU. The load driver outputs are arranged in the primary scram logic circuitry, which is between the scram solenoids and scram solenoid 120 VAC power source. When in a tripped state, the load drivers within a division interconnect with the OLU of all other divisions to form an arrangement (connected in series and in parallel in two separate groups) that results in two-out-of-four scram logic. Reactor scram occurs if load drivers associated with any two or more divisions receive trip signals from the OLUs.

Output contactors are used for back-up scram actuators, scram-follow initiation, and scram reset permissive actuators. When in a tripped state, the output contactors cause the backup scram valve solenoids to energize. The output contactors of the backup scram are arranged in a two-out-of-four configuration similar to that described above for the primary scram load drivers. Backup scram is diverse in power source and function to primary scram.

A manual switch associated with each Division of Trip Actuators provides means to reset the seal-in at the input of all trip actuators in the same division. The reset does not have any effect if the conditions that caused the division trip have not cleared when a reset is attempted. All manual resets are inhibited for ten seconds to allow sufficient time for scram completion.

OPERABILITY requirements for the load drivers are addressed in LCO 3.3.1.2. OPERABILITY requirements for the backup scram output contactors are not addressed within the Technical Specifications.

BASES

BACKGROUND (continued)

Divisions of Manual Scram Controls

OPERABILITY requirements for the Divisions of Manual Scram Controls are addressed in LCO 3.3.1.3, "Reactor Protection System (RPS) Manual Trip Actuation."

Divisions of Scram Logic Circuitry

The two divisions of primary scram logic circuitry are powered from independent and separate power sources. One of the two divisions of scram logic circuitry distributes division 1 safety-related 120 VAC power to the A solenoids of the hydraulic control units (HCUs). The other division of scram logic circuitry distributes division 2 safety-related 120 VAC power to the B solenoids of the HCUs. The HCUs (which include the scram pilot valves and the scram valves, including their solenoids) are, components of the CRD system. A full scram of control rods associated with a particular HCU occurs when both A and B solenoid of the HCU are de-energized.

One scram pilot valve is located in the Hydraulic Control Unit (HCU) for each control rod drive pair. Each scram pilot valve is operated by two solenoids, with both solenoids normally energized. The scram pilot valve controls the air supply to the scram inlet valve for the associated control rod drive pair. When either of two scram pilot valve solenoids is energized, air pressure holds the scram valve closed and therefore, both scram pilot valve solenoids must be de-energized to cause a control rod pair to scram. The scram valve controls the supply for the control rod drive (CRD) water during a scram.

OPERABILITY requirements for components of the Divisions of Scram Logic Circuitry are addressed in LCO 3.1.3, "Control Rod OPERABILITY."

The RPS is designed to provide reliable single-failure proof capability to automatically or manually initiate a reactor scram while maintaining protection against unnecessary scrams resulting from single failures. The RPS satisfies the single-failure criterion even when one entire division of sensors is bypassed and/or when one of the four automatic RPS trip logic divisions is out of service.

BASES

BACKGROUND (continued)

The AC electrical power required by the four divisions of RPS is supplied from four pairs of physically separate and electrically independent uninterruptible safety-related 120 VAC buses. Each RPS division uses the two independent power sources from the same division. Either source of power per division can support the associated RPS division.

Functional diversity is provided by monitoring a wide range of dependent and independent parameters. The input parameters to the scram logic are from instrumentation that monitors reactor vessel water level, reactor vessel steam dome pressure, neutron flux, main steam line isolation valve (MSIV) position, drywell pressure, scram accumulator charging water header pressure, turbine stop valve position, turbine control valve closure, main condenser vacuum, bus voltage, and suppression pool temperature, as well as reactor mode switch in shutdown position and manual scram signals. The reactor mode switch in shutdown position and manual scram signal inputs to the scram logic are addressed in LCO 3.3.1.3.

All average power range monitor (APRM)/oscillation power range monitor (OPRM) and startup range neutron monitor (SRNM) trip decisions are made within the Neutron Monitoring System (NMS). This is done on a divisional basis and the results are then sent directly to the TLUs. Thus, each NMS division sends only two inputs to the divisional TLUs, one for APRM/OPRM trip/no-trip and one for SRNM trip/no-trip. A divisional APRM/OPRM or SRNM may be tripped due to any of the monitored variables exceeding its trip setpoint. The RPS two-out-of-four trip decision is then made, not on a per variable basis, but on an APRM/OPRM tripped or SRNM tripped basis, by looking at the four divisions of APRM/OPRM and four divisions of SRNM. All bypasses of the SRNMs and APRMs/OPRMs are performed within and by the NMS. Refer to LCO 3.3.1.4, "Neutron Monitoring System (NMS) Instrumentation," and LCO 3.3.1.5, "Neutron Monitoring System (NMS) Actuation," for the NMS specifications.

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

The actions of the RPS are assumed in the safety analyses of Reference 2. The RPS initiates a reactor scram when monitored parameter values exceed predetermined values specified in the SCP to preserve the integrity of the fuel cladding, preserve the integrity of the reactor coolant pressure boundary, and preserve the integrity of the containment by minimizing the energy that must be absorbed following a LOCA.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

RPS Instrumentation satisfies the requirements of Selection Criterion 3 of 10 CFR 50.36(c)(2)(ii). Functions not specifically credited in the accident analysis are retained for the overall redundancy and diversity of the RPS as required by the NRC approved licensing basis.

The OPERABILITY of the RPS is dependent on the OPERABILITY of the individual RPS instrumentation Functions specified in Table 3.3.1.1-1. Each Function must have the required number of OPERABLE channels, with their setpoints in accordance with the SCP, where appropriate. The actual setpoint is calibrated consistent with the SCP. Each channel must also respond within its assumed response time.

$NTSP_F$s are specified in the SCP, as required by Specification 5.5.11. The $NTSP_F$s are selected to ensure the actual setpoints are conservative with respect to the Allowable Value between successive CHANNEL CALIBRATIONS. Operation with a trip setpoint less conservative than the $NTSP_F$, but conservative with respect to its Allowable Value, is acceptable. A channel is inoperable if its actual trip setpoint is non-conservative with respect to its required Allowable Value.

The OPERABILITY of RPS Actuation, manual scram features, the NMS features, and scram pilot valves and associated solenoids, and backup scram valves, described in the Background section, are not addressed by this LCO.

The individual Functions are required to be OPERABLE in the MODES specified in the Table which may require an RPS trip to mitigate the consequences of a design basis accident or transient. To ensure a reliable scram function, a combination of Functions is required in each MODE.

RPS is required to be OPERABLE in MODES 1 and 2, and MODE 6 with any control rod withdrawn from a core cell containing one or more fuel assemblies. During normal operation in MODES 3, 4, and 5, all control rods are fully inserted and the Reactor Mode Switch - Shutdown Position control rod withdrawal block (LCO 3.3.2.1, "Control Rod Block Instrumentation") does not allow any control rod to be withdrawn. In MODE 6, control rods withdrawn from a core cell containing no fuel assemblies do not affect the reactivity of the core and therefore are not required to have the capability to scram. Provided all control rods

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

otherwise remain inserted, the RPS function is not required. In this condition the required SDM (LCO 3.1.1,"SHUTDOWN MARGIN") and refuel position one-rod/rod-pair-out interlock (LCO 3.9.2, "Refuel Position One-Rod/Rod-Pair-Out Interlock") ensure no event requiring RPS will occur. Under these conditions, the RPS function is not required to be OPERABLE.

The specific Applicable Safety Analyses, LCO and Applicability discussions are listed below on a Function-by-Function basis.

This Specification covers the RPS instrumentation that encompasses the sensor channels up through the DTMs.

Although there are four channels of RPS instrumentation for each function, only three channels of RPS instrumentation for each function are required to be OPERABLE. The three required channels are those channels associated with the DC and Uninterruptible AC Electrical Power Distribution Divisions required by LCO 3.8.6, "Distribution Systems - Operating," and LCO 3.8.7, "Distribution Systems - Shutdown." This is acceptable because the single-failure criterion is met with three OPERABLE RPS instrumentation channels, and because each RPS division is associated with and receives power from only one of the four electrical divisions.

<u>1. Neutron Monitor System Input - Startup Range Neutron Monitors</u>

The SRNM is a part of the NMS. The NMS Functions associated with the SRNM are described in the Bases of LCO 3.3.1.4. The SRNM provides diverse protection for the Rod Worth Minimizer (RWM) in the Rod Control and Information System (RC&IS), which monitors and controls the movement of control rods at low power. The RWM prevents the withdrawal of an out-of-sequence control rod during startup that could result in an unacceptable neutron flux excursion (Ref. 3). The SRNM provides mitigation of the neutron flux excursion in the control rod withdrawal event during startup (Ref. 4).

The SRNMs are also capable of limiting other reactivity excursions during startup, such as cold-water injection events, although no credit is specifically assumed.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

Three channels of Neutron Monitoring System Input - Startup Range Neutron Monitors are required to be OPERABLE to ensure no single instrument failure will preclude a scram from this Function on a valid signal.

This Function is required to be OPERABLE in the MODES where the SRNM Functions are required.

2. Neutron Monitor System Input - Average Power Range Monitors /Oscillation Power Range Monitors (OPRMs)

The APRMs and OPRMs are a part of the NMS. The NMS Functions associated with the APRMs and OPRMs are described in the Bases of LCO 3.3.1.4.

Three channels of NMS inputs from the NMS (APRMs/OPRMs) arranged in a two-out-of-four logic are required to be OPERABLE to ensure no single instrument failure will preclude a scram from this Function on a valid signal.

This Function is required to be OPERABLE in the MODES where the APRM and OPRM Functions are required (LCO 3.3.1.4).

3. Scram Accumulator Charging Water Header Pressure - Low-Low

To maintain the continuous ability to scram, the scram accumulator charging water header maintains the hydraulic scram accumulators at a high pressure. The scram valves under this condition remain closed, so that no flow passes through the scram accumulator charging water header. Pressure in the scram accumulator charging water header is monitored. The Scram Accumulator Charging Water Header Pressure - Low-Low Function initiates a scram if a significant degradation in the scram accumulator charging water header pressure occurs. During a scram, the water discharge from the accumulators goes into the reactor, and thus against reactor pressure. Therefore, fully charged hydraulic control units (HCUs) are essential for assuring reactor scram. After a reactor scram, this Function can be bypassed from the operator's console to reset the RPS, allowing the scram valves to close and the HCUs to be re-pressurized.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

Low-Low scram accumulator charging water header pressure signals are initiated from four pressure sensors located at the scram accumulator charging water header. The Scram Accumulator Charging Water Header Pressure - Low-Low Allowable Value is chosen to provide sufficient margin to the capability to scram.

Three channels of Scram Accumulator Charging Water Header Pressure - Low-Low Function are required to be OPERABLE to ensure no single instrument failure will preclude a scram from this Function on a valid signal. The Function is required to be OPERABLE when the scram capability is required in MODES 1 and 2, and MODE 6 with any control rod withdrawn from a core cell containing one or more fuel assemblies.

4. Reactor Vessel Steam Dome Pressure - High

An increase in the Reactor Pressure Vessel (RPV) pressure during reactor operation compresses the steam voids and results in a positive reactivity insertion. This causes the neutron flux and THERMAL POWER transferred to the reactor coolant to increase, which could challenge the integrity of the fuel cladding and the integrity of the Reactor Coolant System (RCS) pressure boundary. No specific safety analysis takes direct credit for this Function. However, the Reactor Vessel Steam Dome Pressure - High Function initiates a scram for transients that result in a pressure increase, counteracting the pressure increase by rapidly reducing core power. For the overpressurization protection analysis, the APRM Fixed Neutron Flux - High Function is assumed to terminate the MSIV Closure event and, along with the safety relief valves, limits the peak RPV pressure to less than the ASME Code limits.

High reactor pressure signals are initiated from four pressure sensors that sense reactor pressure. The Reactor Vessel Steam Dome Pressure - High Allowable Value is chosen to provide a sufficient margin to the ASME Section III Code limits during the event.

Three channels of Reactor Vessel Steam Dome Pressure - High Function are required to be OPERABLE to ensure no single instrument failure will preclude a scram from this Function on a valid signal. The Function is required to be OPERABLE in MODES 1 and 2 when the Reactor Coolant System is pressurized and the potential for pressure increase exists.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

5. Reactor Vessel Water Level - Low, Level 3

Low Reactor Vessel (RPV) water level indicates the capability to cool the fuel may be threatened. Should RPV water level decrease too far, fuel damage could result. Therefore, a reactor scram is initiated at Level 3 to substantially reduce the heat generated in the fuel from fission. The Reactor Vessel Water Level - Low, Level 3 Function is assumed to be available in various design basis line break analyses and in loss of feedwater events, however it is a secondary scram signal to Loss of Power Generation Bus. The reactor scram reduces the amount of energy required to be absorbed and assures that the fuel peak cladding temperature remains below the limits of 10 CFR 50.46.

Reactor Vessel Water Level - Low, Level 3, signals are initiated from four differential pressure sensors that sense the difference between the pressure due to a constant column of water (reference leg) and the pressure due to the actual water level (variable leg) in the vessel.

Three channels of Reactor Vessel Water Level - Low, Level 3, Function are required to be OPERABLE to ensure no single instrument failure will preclude a scram from this Function on a valid signal.

The Reactor Vessel Water Level - Low, Level 3 Allowable Value is selected to ensure that for transients involving loss of all normal feedwater flow, the core will not be uncovered.

The Function is required in MODES 1 and 2 where considerable energy exists in the reactor coolant system resulting in the limiting transients and accidents.

6. Reactor Vessel Water Level - High, Level 8

High RPV water level indicates a potential problem with the feedwater level control system, resulting in the addition of reactivity associated with the introduction of a significant amount of relatively cold feedwater. Therefore, a scram is initiated at Level 8 to ensure the safety analyses are met. The Reactor Vessel Water Level - High, Level 8 Function is directly assumed in the analysis of feedwater controller failure, maximum demand (Ref. 5).

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

Reactor Vessel Water Level - High, Level 8, signals are initiated from four differential pressure sensors that sense the difference between the pressure due to a constant column of water (reference leg) and the pressure due to the actual water level (variable leg) in the vessel. The Reactor Vessel Water Level - High, Level 8 Allowable Value is specified to ensure the safety analyses criteria are met.

Three channels of the Reactor Vessel Water Level - High, Level 8, are required to be OPERABLE when THERMAL POWER is ≥ 25% RTP to ensure no single instrument failure will preclude a scram from this Function on a valid signal. With THERMAL POWER < 25% RTP, this Function is not required since MCPR is not a concern below 25% RTP.

7. Main Steam Isolation Valve - Closure (Per Steam Line)

Main Steam Isolation Valve (MSIV) closure results in loss of the main turbine and the condenser as a heat sink for the nuclear steam supply system and indicates a need to shut down the reactor to reduce heat generation. Therefore, a reactor scram is initiated on a MSIV closure signal before the MSIVs are completely closed in anticipation of the complete loss of the normal heat sink and subsequent overpressurization transient. However, for the overpressurization protection analysis of Reference 6, the Average Power Range Monitor Fixed Neutron Flux - High Function, along with the safety relief valves, limits the peak RPV pressure to less than the ASME Code limits. That is, the direct scram on position switches for MSIV closure events is not assumed in the overpressurization analysis. Additionally, MSIV closure is assumed in the transients analyzed in References 7 and 8 . The reactor scram reduces the amount of energy required to be absorbed and, along with the actions of the Isolation Condenser System (ICS), assures that the safety analyses assumptions are met.

MSIV closure signals are initiated from position switches located on each of the eight MSIVs. On each MSL, two position switches are mounted on the inboard MSIV and two position switches are mounted on the outboard MSIV. Each of the position switches on any one MSL is associated with a different RPS divisional sensor channel. The logic for the Main Steam Isolation Valve - Closure Function is arranged such that either the inboard or outboard valve on two or more of the main steam lines (MSLs) must close in order for a scram to occur.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

The Main Steam Isolation Valve - Closure (per Steam Line) Function Allowable Value is specified to ensure that a scram occurs prior to a significant reduction in steam flow, thereby reducing the severity of the subsequent pressure transient.

Three channels of Main Steam Isolation Valve - Closure (per Steam Line) Function are required to be OPERABLE to ensure no single instrument failure will preclude the scram from this Function on a valid signal. This Function is only required in MODE 1 because with the MSIVs open and the heat generation rate high, a pressurization transient can occur if the MSIVs close. In MODE 2 the heat generation rate is low enough that the other diverse RPS Functions provide sufficient protection.

8. Drywell Pressure - High

High pressure in the drywell could indicate a break in the Reactor Coolant System pressure boundary. A reactor scram is initiated to minimize the possibility of fuel damage and to reduce the amount of energy being added to the coolant and to the drywell. The Drywell Pressure - High Function is assumed to be available for LOCA events inside the drywell and is credited in the inadvertent operation of a depressurization valve. High drywell pressure signals are initiated from four pressure sensors that sense drywell pressure. The Allowable Value was selected to be as low as possible and be indicative of a LOCA inside the drywell or an opened depressurization valve.

Three channels of Drywell Pressure - High Function are required to be OPERABLE to ensure no single instrument failure will preclude a scram from this Function on a valid signal. The Function is required in MODES 1 and 2 where considerable energy exists in the reactor coolant system resulting in the limiting transients and accidents.

9. Suppression Pool Temperature - High

High temperature in the suppression pool could indicate a break in the RCS pressure boundary or an opened safety relief valve. A reactor scram is initiated to reduce the amount of energy being added to the containment. The Suppression Pool Temperature - High Function is taken credit for in the analysis of an inadvertent opening of a safety relief valve (Ref. 9).

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

High suppression pool temperature signals are initiated from four divisions of temperature sensors located in the suppression pool. Four channels of safety-related divisional temperature signals, each formed by the average value of a group of thermocouples installed evenly inside the suppression pool, provide the suppression pool temperature data for automatic scram initiation. When the established limits of high temperature are exceeded in two of the four divisions, a scram initiation and indication signals are generated. The temperature sensors provide analog output signals to the RMU, which in turn provides the equivalent digital signal to the appropriate DTM. The temperature sensors are components of the Containment Monitoring System (CMS). The suppression pool water level signals are provided along with the suppression pool temperature signals. When water level drops below selected temperature sensors, the exposed sensors are logically bypassed such that only sensors below the water level are utilized to determine the averaged temperature signal to the RPS.

The Allowable Value was selected considering the maximum operating temperature and to be indicative of an inadvertently opened safety relief valve.

Three channels of Suppression Pool Temperature - High Function are required to be OPERABLE to ensure no single instrument failure will preclude a scram from this Function on a valid signal. There are a total of 64 suppression pool temperature switches that make up the four channels of Suppression Pool Temperature - High Function (16 suppression pool temperature switches per channel). For a channel of the Suppression Pool Temperature - High Function to be OPERABLE, 12 of the 16 assigned Suppression Pool Temperature switches must be OPERABLE. The Function is required in MODES 1 and 2 where considerable energy exists in the reactor coolant system.

10. Turbine Stop Valve - Closure

Closure of the turbine stop valves (TSV) results in the loss of a heat sink that produces reactor pressure, neutron flux, and heat flux transients that must be limited. Therefore, a reactor scram is initiated at the start of TSV closure in anticipation of the transients that would result from the closure of these valves with insufficient turbine bypass valve capacity available. The Turbine Stop Valve - Closure Function is the primary scram signal for the turbine trip event analyzed in Reference 10. For this event, the reactor scram reduces the amount of energy required to be absorbed and ensures that the fuel cladding integrity Safety Limit is not exceeded.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

Turbine Stop Valve - Closure signals are initiated by the separate valve stem position switches on each of the four turbine stop valves. Each position switch provides an open/close contact output signal through hard-wired connections to the DTM in one of the four RPS sensor channels. The Turbine Stop Valve – Closure trip occurs in each division of trip logic when any two or more position switches detect the turbine stop valve closure. The Function is enabled at THERMAL POWER > 40% RTP. This is accomplished automatically by an analog simulated thermal power signal from the NMS. This Function is also automatically bypassed if sufficient turbine bypass valves are open within a preset time delay after the initiation of the trip signal. The analog simulated thermal power signal from NMS is also used to determine the required bypass capacity.

The Turbine Stop Valve - Closure Allowable Value is selected to be high enough to detect imminent TSV closure thereby reducing the severity of the subsequent pressure transient.

Three channels of Turbine Stop Valve - Closure Function are required to be OPERABLE to ensure that no single instrument failure will preclude a scram from this Function even if one TSV should fail to close. This Function is required, consistent with analysis assumptions, whenever THERMAL POWER is ≥ 40% RTP. This Function is not required when THERMAL POWER is < 40% RTP since the Reactor Steam Dome Pressure - High and the Average Power Range Monitor Fixed Neutron Flux - High Functions are adequate to maintain the necessary safety margins.

11. Turbine Control Valve Fast Closure, Trip Oil Pressure - Low

Fast closure of the turbine control valves (TCVs) results in the loss of a heat sink that produces reactor pressure, neutron flux, and heat flux transients that must be limited. Therefore, a reactor scram is initiated on TCV fast closure in anticipation of the transients that would result from the closure of these valves with insufficient turbine bypass valve capacity available. The Turbine Control Valve Fast Closure, Trip Oil Pressure - Low Function is the primary scram signal for the generator load rejection event analyzed in Reference 11. For this event, the reactor scram reduces the amount of energy required to be absorbed and ensures that the fuel cladding integrity Safety Limit is not exceeded.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

Turbine Control Valve Fast Closure, Trip Oil Pressure - Low signals are initiated by the hydraulic trip system pressure at each control valve. There is one pressure sensor associated with each control valve. Each pressure sensor provides a signal through hard-wired connections to the DTM in each of the four RPS sensor channels. This Function must be enabled at THERMAL POWER ≥ 40% RTP. This is accomplished automatically by an analog simulated thermal power signal from NMS. This Function is automatically bypassed if sufficient turbine bypass valves are open within a preset time delay after the initiation of the trip signal. The analog simulated thermal power signal from NMS is also used to determine the required bypass capacity.

The Turbine Control Valve Fast Closure, Trip Oil Pressure - Low Allowable Value is selected high enough to detect imminent TCV fast closure.

Three channels of Turbine Control Valve Fast Closure, Trip Oil Pressure - Low Function, are required to be OPERABLE to ensure that no single instrument failure will preclude a scram from this Function on a valid signal. This Function is required, consistent with the analysis assumptions, whenever THERMAL POWER is ≥ 40% RTP. This Function is not required when THERMAL POWER is < 40% RTP since the Reactor Vessel Steam Dome Pressure - High and the Average Power Range Monitor Fixed Neutron Flux - High Functions are adequate to maintain the necessary safety margins.

12. Main Condenser Pressure - High

The Main Condenser Pressure - High Function is provided to help ensure the fuel cladding integrity Safety Limit is not exceeded by reducing the core energy in anticipation that the high condenser pressure will also trip the main turbine and prevent bypass valve operation. The Main Condenser Pressure - High Function is the primary scram signal for the loss of condenser vacuum event analyzed in Reference 12. For this event, the reactor scram reduces the amount of energy required to be absorbed by the main condenser and helps to ensure the fuel cladding integrity Safety Limit is not exceeded by reducing the core energy prior to the fast closure of the turbine stop valves. The reactor scram at Main Condenser Pressure - High will initiate to shut off steam flow to the main condenser to protect the main turbine and to avoid the potential for rupturing the low-pressure turbine casing.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

Main condenser pressure signals are derived from four pressure sensors that sense the pressure in the condenser. Each pressure sensor provides an analog output signal through hard-wired connections to the DTM in each of the four RPS sensor channels. The Allowable Value was selected to reduce the severity of a loss of main condenser vacuum event by anticipating the transient and scramming the reactor at a higher vacuum than the setpoints that close the turbine stop valves and bypass valves.

Three channels of Main Condenser Pressure - High Function are required to be OPERABLE to ensure that no single instrument failure will preclude a scram from this Function on a valid signal. The Function is required in MODE 1 since, in this MODE, a significant amount of core energy can be rejected to the main condenser.

13. Power Generation Bus Loss

The plant electrical system has four redundant power generation buses that operate at 13.8 kV. These buses supply power for the feedwater pumps and circulating pumps. In MODE 1, at least three of the four buses must be powered. Power generation bus loss signals are derived from four voltage sensors. If the voltage sensor (one per division) on each bus senses a low voltage below the required level, indicating that less than three buses are operating above the requirement level, a scram is initiated after a preset delay time. This delay time is to accommodate for the auto-transfer from the Unit Auxiliary Transformer (UAT) feed to the Reserve Auxiliary Transformer (RAT) feed. When the power generation buses are not operating at or above the required level, the feedwater pumps would be tripped and feedwater flow would be lost. Purpose of this scram on losing feedwater flow is to mitigate the reactor water level drop to Level 1 following the loss of feedwater pump function. This scram will terminate additional steam production within the vessel before Level 3 is reached.

The Allowable Value was selected high enough to detect a loss of voltage in order to mitigate the reactor water level drop to Level 1 following the loss of feedwater pump function.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

Three channels of Power Generation Bus Loss Function are required to be OPERABLE to ensure that no single instrument failure will preclude a scram from this Function on a valid signal. The Function is required in MODE 1 where considerable energy exists in the reactor coolant system resulting in the limiting transients and accidents. During MODE 2, 3, 4, 5, and 6, the core energy is significantly lower.

14. Feedwater Temperature Biased Simulated Thermal Power – High

The Feedwater Temperature Biased Simulated Thermal Power – High Function is provided to help ensure the fuel cladding Safety Limit is not exceeded in the event of a significant decrease in feedwater temperature (Ref. 13). Feedwater temperature is measured by four separate temperature sensors mounted on each FW line. Each feedwater temperature sensor is connected to a separate RPS instrumentation channel and is associated with a separate RPS electrical division. The RPS uses feedwater temperature to generate a simulated thermal power trip setpoint that is a function of feedwater temperature.

Three channels of the Feedwater Temperature Biased Simulated Thermal Power – High Function are required to be OPERABLE when THERMAL POWER is ≥ 25% RTP to ensure that no single instrument failure will preclude a scram from this Function on a valid signal. With THERMAL POWER < 25% RTP, this Function is not required since MCPR is not a concern below 25% RTP.

15. Simulated Thermal Power Biased Feedwater Temperature – High

The Simulated Thermal Power Biased Feedwater Temperature – High Function is provided to help ensure the fuel cladding Safety Limit is not exceeded in the event of a significant decrease in feedwater temperature (Ref. 13). Feedwater temperature is measured by four separate temperature sensors mounted on each FW line. Each feedwater temperature sensor is connected to a separate RPS instrumentation channel and is associated with a separate RPS electrical division. The RPS uses the simulated thermal power signal from NMS to generate a feedwater temperature trip setpoint that is a function of simulated thermal power.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

Three channels of the Simulated Thermal Power Biased Feedwater Temperature – High Function are required to be OPERABLE when THERMAL POWER is ≥ 25% RTP to ensure that no single instrument failure will preclude a scram from this Function on a valid signal. With THERMAL POWER < 25% RTP, this Function is not required since MCPR is not a concern below 25% RTP.

<u>16. Simulated Thermal Power Biased Feedwater Temperature – Low</u>

The Simulated Thermal Power Biased Feedwater Temperature – Low Function is provided to help ensure the fuel cladding Safety Limit is not exceeded in the event of a significant decrease in feedwater temperature (Ref. 13). Feedwater temperature is measured by four separate temperature sensors mounted on each FW line. Each feedwater temperature sensor is connected to a separate RPS instrumentation channel and is associated with a separate RPS electrical division. The RPS uses the simulated thermal power signal from NMS to generate a feedwater temperature trip setpoint that is a function of simulated thermal power.

Three channels of the Simulated Thermal Power Biased Feedwater Temperature – Low Function are required to be OPERABLE when THERMAL POWER is ≥ 25% RTP to ensure that no single instrument failure will preclude a scram from this Function on a valid signal. With THERMAL POWER < 25% RTP, this Function is not required since MCPR is not a concern below 25% RTP.

ACTIONS

A Note has been provided to modify the ACTIONS related to RPS Instrumentation channels. Section 1.3, Completion Times, specifies once a Condition has been entered, subsequent divisions, subsystems, components or variables expressed in the Condition discovered to be inoperable or not within limits, will not result in separate entry into the Condition. Section 1.3 also specifies Required Actions of the Condition continue to apply for each additional failure, with Completion Times based on initial entry into the condition. However, the Required Actions for inoperable RPS Instrumentation channels provide appropriate compensatory measures for separate inoperable channels. As such, a Note has been provided which allows separate Condition entry for each inoperable RPS Instrumentation channel.

BASES

ACTIONS (continued)

A.1

The 12-hour Completion Time is acceptable based on engineering judgment considering the diversity of sensors available to provide trip signals, the redundancy of the RPS design, and the low probability of an event requiring a reactor scram during this interval. However, this out of service time is only acceptable provided the associated Function still maintains RPS trip capability (refer to Required Action B.1 Bases). If the inoperable instrumentation channel cannot be restored to OPERABLE status within the 12-hour Completion Time, the associated instrument channel must be verified to be in trip. This is acceptable because verifying the affected RPS instrument channel in trip conservatively compensates for the inoperability by placing the RPS in a one-out-of-two configuration, restoring the capability to accommodate a single failure.

Alternatively, if it is not desirable to verify the associated instrument channel in trip (as in the case where it is desired to place the affected channel of sensors in bypass), Condition B must be entered and its Required Action taken when the Completion Time of Required Action A.1 expires.

B.1

Required Action B.1 directs entry into the appropriate Condition referenced in Table 3.3.1.1-1 if the Required Action and Completion Time of Condition A are not met or if multiple, inoperable, untripped required channels (i.e., two or more required channels for most Functions) for the same Function result in the Function not maintaining RPS trip capability. A Function is considered to be maintaining RPS trip capability when sufficient channels are OPERABLE or in trip such that the RPS logic will generate a trip signal from the given Function on a valid signal.

The applicable Condition specified in the Table is Function and MODE or other specified condition dependent and may change as the Required Action of a previous Condition is completed.

BASES

ACTIONS (continued)

C.1, D.1, E.1, F.1, and G.1

If the required RPS instrumentation channel(s) is not restored to OPERABLE status, or the affected instrumentation channel is not in trip within the allowed Completion Time, or if RPS trip capability is not maintained, the plant must be placed in a MODE or other specified condition in which the LCO does not apply. The Completion Times are reasonable, based on operating experience, to reach the specified condition from full power conditions in an orderly manner and without challenging plant systems. In addition, the Completion Time of Required Actions C.1 and D.1 are consistent with the Completion Time provided in LCO 3.2.2, "MINIMUM CRITICAL POWER RATIO (MCPR)."

SURVEILLANCE REQUIREMENTS

As noted at the beginning of the SRs, the SRs for each RPS instrumentation Function are located in the SRs column of Table 3.3.1.1-1.

SR 3.3.1.1.1

Performance of the CHANNEL CHECK once every 12 hours ensures that a gross failure of instrumentation has not occurred.

The RPS is cyclically tested from the sensor input point to the logic contact output by online self-diagnostics. The self-diagnostic capabilities include microprocessor checks, system initialization, watchdog timers, memory integrity checks, input/output (I/O) data integrity checks, communication bus interface checks, and checks on the application program (checksum).

A CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

Agreement criteria are determined by the plant staff, based on a combination of the channel instrument uncertainties, including indication and readability. If a channel is outside the criteria, it may be an indication that the instrument has drifted outside its limit.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The Frequency is based upon operating experience that demonstrates channel failure is rare. The CHANNEL CHECKs every 12 hours supplement less formal, but more frequent, checks of channels during normal operational use of the displays associated with the channels required by the LCO.

SR 3.3.1.1.2

A CHANNEL FUNCTIONAL TEST is performed on each required channel to ensure that the entire channel will perform the intended function. This test ensures a complete CHANNEL FUNCTIONAL TEST of required instrument channels from the sensor input through the DTM function.

The RPS is cyclically tested from the sensor input point to the logic contact output by online self-diagnostics. The self-diagnostic capabilities include microprocessor checks, system initialization, watchdog timers, memory integrity checks, input/output (I/O) data integrity checks, communication bus interface checks, and checks on the application program (checksum).

The Frequency of 31 days is based on the reliability of the channels.

SR 3.3.1.1.3

A CHANNEL CALIBRATION is a complete check of the instrument loop and the sensor. This test verifies the required channel responds to the measured parameter within the necessary range and accuracy.

CHANNEL CALIBRATION leaves the required channel adjusted to the $NTSP_F$ within the "as-left" tolerance to account for instrument drifts between successive calibrations consistent with the methods and assumptions required by the SCP.

The Frequency is based upon the assumption of a 24-month calibration interval in the determination of the magnitude of equipment drift in the setpoint analysis.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.1.1.4

This SR ensures that the individual required channel response times are less than or equal to the maximum values assumed in the accident analysis. The RPS RESPONSE TIME acceptance criteria are included in Reference 14.

RPS RESPONSE TIME may be verified by actual response time measurements in any series of sequential, overlapping, or total channel measurements. This test encompasses the sensor channels up through the DTMs and overlaps the testing required by SR 3.3.1.2.2 to ensure complete testing of instrument channels and actuation circuitry.

COL 16.0-1-A 3.3.1.1-2

[However, some sensors for Functions are allowed to be excluded from specific RPS RESPONSE TIME measurement if the conditions of Reference XX are satisfied. If these conditions are satisfied, sensor response time may be allocated based on either assumed design sensor response time or the manufacturer's stated design response time. When the requirements of Reference XX are not satisfied, sensor response time must be measured. Furthermore, measurement of the instrument loop response times is not required if the conditions of Reference XX are satisfied.]

RPS RESPONSE TIME tests are conducted on a 24-month STAGGERED TEST BASIS for three channels. The Frequency of 24 months on a STAGGERED TEST BASIS ensures that the required channels associated with each division are alternately tested. The 24-month test Frequency is consistent with the refueling cycle and with operating experience that shows that random failures of instrumentation components causing serious response time degradation, but not channel failure, are infrequent.

BASES

REFERENCES

1. Chapter 7, Figure 7.2-1.
2. Chapter 15.
3. Subsection 7.7.2.
4. Subsection 15.3.8.
5. Subsection 15.3.2.
6. Subsection 5.2.2.
7. Subsection 15.3.3.
8. Subsection 15.2.2.7.
9. Subsection 15.3.13.
10. Subsection 15.2.2.5.
11. Subsection 15.2.2.3.
12. Subsection 15.2.2.8.
13. Subsection 15.3.1.
14. Section 15.2.

B 3.3 INSTRUMENTATION

B 3.3.1.2 Reactor Protection System (RPS) Actuation

BASES

BACKGROUND

The RPS is designed to initiate a reactor scram when one or more monitored parameters exceed their specified limit, to preserve the integrity of the fuel cladding, preserve the integrity of the reactor coolant pressure boundary, and preserve the integrity of the containment by minimizing the energy that must be absorbed following a LOCA. This can be accomplished either automatically or manually.

A detailed description of the RPS instrumentation and RPS actuation logic is provided in the Bases for LCO 3.3.1.1, “Reactor Protection System (RPS) Instrumentation.”

This Specification provides requirements for the RPS actuation circuitry that consists of the Divisions of Trip Logic (with the exception of OPERABILITY of the digital trip function, which is addressed in LCO 3.3.1.1), and the Divisions of Trip Actuators (except for OPERABILITY of the backup scram load drivers which are not addressed within the Technical Specifications).

APPLICABLE SAFETY ANALYSES

The actions of the RPS are assumed in the safety analyses of Reference 1. The RPS initiates a reactor scram when monitored parameter values exceed the trip setpoints to preserve the integrity of the fuel cladding, preserve the integrity of the reactor coolant pressure boundary, and preserve the integrity of the containment by minimizing the energy that must be absorbed following a LOCA. RPS actuation divisions support the OPERABILITY of the RPS Instrumentation, “LCO 3.3.1.1, Reactor Protection System (RPS) Instrumentation” and therefore are required to be OPERABLE.

RPS Actuation satisfies the requirements of Selection Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

Although there are four RPS automatic actuation divisions, only three RPS automatic actuation divisions are required to be OPERABLE to ensure no single automatic actuation division failure will preclude a scram to occur on a valid signal. The three required divisions are those divisions associated with the DC and Uninterruptible AC Electrical Power Distribution Divisions required by LCO 3.8.6, "Distribution Systems -

BASES

LCO (continued)

Operating," and LCO 3.8.7, "Distribution Systems - Shutdown." This is acceptable because the single-failure criterion is still met with three OPERABLE RPS actuation divisions, and because each RPS division is associated with and receives power from only one of the four electrical divisions. This Specification provides requirements for the RPS actuation circuitry that consists of the Divisions of Trip Logic, and the Divisions of Trip Actuators.

The OPERABILITY of scram pilot valves and associated solenoids, and backup scram valves are not addressed by this LCO. The OPERABILITY of the RPS Instrumentation is covered in LCO 3.3.1.1.

APPLICABILITY

Three RPS automatic actuation divisions are required to be OPERABLE in MODES 1 and 2, and in MODE 6 with any control rod withdrawn from a core cell containing one or more fuel assemblies. During normal operation in MODES 3, 4 and 5, all control rods are fully inserted and the Reactor Mode Switch - Shutdown Position control rod withdrawal block (LCO 3.3.2.1, "Control Rod Block Instrumentation") does not allow any control rod to be withdrawn. In MODE 6, control rods withdrawn from a core cell containing no fuel assemblies do not affect the reactivity of the core and, therefore, are not required to have the capability to scram. Provided all other control rods remain inserted, the RPS function is not required. In this condition, the required SDM (LCO 3.1.1, "SHUTDOWN MARGIN") and refuel position one-rod-out interlock (LCO 3.9.2, "Refuel Position One-Rod/Rod-Pair-Out Interlock") ensure that no event requiring RPS will occur. Under these conditions, the RPS function is not required to be OPERABLE.

ACTIONS

A Note has been provided to modify the ACTIONS related to RPS automatic actuation divisions. Section 1.3, Completion Times, specifies once a Condition has been entered, subsequent divisions, subsystems, components or variables expressed in the Condition discovered to be inoperable or not within limits, will not result in separate entry into the Condition. Section 1.3 also specifies Required Actions of the Condition continue to apply for each additional failure, with Completion Times based on initial entry into the condition. However, the Required Actions for inoperable RPS automatic actuation divisions provide appropriate compensatory measures for separate inoperable divisions. As such, a Note has been provided which allows separate Condition entry for each inoperable RPS automatic actuation division.

BASES

ACTIONS (continued)

A.1

The 12-hour Completion Time is acceptable based on engineering judgment considering the redundancy of the RPS automatic actuation divisions and the low probability of an event requiring reactor scram during this interval. However, this out of service time is only acceptable provided the RPS maintains automatic trip capability (refer to Required Action B.1 Bases). If the inoperable division cannot be restored to OPERABLE status within the 12-hour Completion Time, the affected actuation division must be verified to be in trip. This is acceptable because verifying the affected RPS actuation division in trip conservatively compensates for the inoperability by placing the RPS in a one-out-of-two configuration, restoring the capability to accommodate a single failure.

Alternatively, if it is not desirable to verify the affected actuation division in trip (as in the case where it is desired to place the affected actuation division in bypass), Condition C must be entered and its Required Action taken when the Completion Time of Required Action A.1 expires.

B.1

If any Required Action and associated Completion Time of Condition A is not met in MODE 1 or 2, or if multiple, inoperable, untripped required divisions of RPS actuation (i.e., two or more required divisions) result in the RPS automatic actuation capability not maintained in MODE 1 or 2, the plant must be brought to a MODE in which the LCO does not apply. RPS automatic actuation capability is considered to be maintained when sufficient required actuation divisions are OPERABLE or in trip such that the RPS logic will generate a trip signal on a valid signal. To achieve this status, the plant must be brought to MODE 3 within 12 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 safety systems.

C.1

With automatic actuation capability not maintained in MODE 6 or if any Required Action and associated Completion Time of Condition A is not met in MODE 6, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must immediately initiate action to fully insert all insertable control rods in core cells containing one or more fuel assemblies. Action must continue until all such control rods

BASES

ACTIONS (continued)

are fully inserted. Control rods in core cells containing no fuel assemblies do not affect the reactivity of the core and, therefore, do not have to be inserted.

SURVEILLANCE REQUIREMENTS

SR 3.3.1.2.1

The LOGIC SYSTEM FUNCTIONAL TEST demonstrates the OPERABILITY of the RPS Actuation divisions, including the two-out-of-four function of the Trip Logic Unit (TLU), Output Logic Unit (OLU), and Load Drivers (LDs) for a specific division. The functional testing of control rods, in LCO 3.1.3, overlaps this Surveillance to provide complete testing of the assumed safety function.

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 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 24-month Frequency.

SR 3.3.1.2.2

This SR ensures that the individual required division response times are less than or equal to the maximum values assumed in the accident analysis. The RPS RESPONSE TIME acceptance criteria are included in Reference 2.

COL 16.0-1-A 3.3.1.2-1

[However, some portions of the RPS actuation circuitry are allowed to be excluded from specific RPS RESPONSE TIME measurement if the conditions of Reference XX are satisfied. Furthermore, measurement of the instrument loop response times is not required if the conditions of Reference XX are satisfied.]

RPS RESPONSE TIME may be verified by actual response time measurements in any series of sequential, overlapping, or total channel measurements. This test encompasses the RPS actuation circuitry that consists of the Divisions of Trip Logic, and the Divisions of Trip Actuators and overlaps the testing required by SR 3.3.1.1.4 to ensure complete testing of instrument channels and actuation circuitry.

SURVEILLANCE REQUIREMENTS (continued)

RPS RESPONSE TIME tests are conducted on a 24-month STAGGERED TEST BASIS for three divisions. The Frequency of 24 months on a STAGGERED TEST BASIS ensures that each required division is alternately tested. The 24-month test Frequency is consistent with the refueling cycle and with operating experience that shows that random failures of instrumentation components causing serious response time degradation, but not channel failure, are infrequent.

REFERENCES

1. Chapter 15.
2. Section 15.2.

B 3.3 INSTRUMENTATION

B 3.3.1.3 Reactor Protection System (RPS) Manual Actuation

BASES

BACKGROUND

The RPS is designed to initiate a reactor scram when one or more monitored parameters exceed their specified limit, to preserve the integrity of the fuel cladding and the Reactor Coolant System (RCS), and minimize the energy that must be absorbed following a loss of coolant accident (LOCA). This can be accomplished either automatically or manually.

Manual scram is accomplished either via two manual scram push buttons (Division 1 and Division 2 manual actuation channels) or by placing the reactor mode switch in the shutdown position. The reactor mode switch is a single switch that initiates a scram when the switch is in the shutdown position by interrupting power to the circuits affected by each manual scram pushbutton (Division 1 and Division 2 Reactor Mode Switch - Shutdown actuation channels). The two manual scram pushbuttons each de-energize a separate path for the four scram groups such that when individually actuated a half-scram condition results, and when actuated together a full scram results. Placing the mode switch in shutdown immediately results in full scram by interrupting power to the circuits affected by each manual scram pushbutton. If a full scram occurs, scram reset is prevented for 10 seconds. This 10-second delay on reset ensures that the scram function will be completed.

One scram pilot valve is located in the Hydraulic Control Unit (HCU) for each control rod drive pair. Each scram pilot valve is operated by two solenoids, with both solenoids normally energized. The scram pilot valve controls the air supply to the scram inlet valve for the associated control rod drive pair. When either of two scram pilot valve solenoids is energized, air pressure holds the scram valve closed and, therefore, both scram pilot valve solenoids must be de-energized to cause a control rod pair to scram. The scram valve controls the supply for the control rod drive (CRD) water during a scram.

The backup scram valves, which energize on a scram signal to depressurize the scram air header, are also controlled by the RPS.

The OPERABILITY of scram pilot valves and associated solenoids is addressed in LCO 3.1.3, "Control Rod OPERABILITY." OPERABILITY of the backup scram valves is not addressed within the Technical Specifications.

BASES

APPLICABLE SAFETY ANALYSES	RPS Manual Actuation does not satisfy any criteria of 10 CFR 50.36(c)(2)(ii), but is retained for the overall redundancy and diversity of the RPS as required by the NRC-approved licensing basis.
LCO	Two manual actuation channels and two Reactor Mode Switch - Shutdown actuation channels as specified in Table 3.3.1.3-1 are required to be OPERABLE to retain the overall redundancy and diversity of the RPS.
APPLICABILITY	The manual actuation Functions are required to be OPERABLE whenever the RPS automatic instrumentation is required to be OPERABLE in LCO 3.3.1.1, "Reactor Protection System (RPS) Instrumentation"). RPS is required to be OPERABLE in MODES 1 and 2, and MODE 6 with any control rod withdrawn from a core cell containing one or more fuel assemblies. During normal operation in MODES 3, 4, and 5, all control rods are fully inserted and the Reactor Mode Switch - Shutdown Position control rod withdrawal block (LCO 3.3.2.1, "Control Rod Block Instrumentation") does not allow any control rod to be withdrawn. In MODE 6, control rods withdrawn from a core cell containing no fuel assemblies do not affect the reactivity of the core and therefore are not required to have the capability to scram. Provided all control rods otherwise remain inserted, the RPS function is not required. In this condition the required SDM (LCO 3.1.1,"SHUTDOWN MARGIN") and refuel position one-rod-out/rod-pair-out interlock (LCO 3.9.2, "Refuel Position One-Rod/Rod-Pair-Out Interlock") ensures no event requiring RPS will occur. Under these conditions, the RPS function is not required to be OPERABLE.
ACTIONS	A Note has been provided to modify the ACTIONS related to RPS manual actuation Functions. Section 1.3, Completion Times, specifies once a Condition has been entered, subsequent divisions, subsystems, components or variables expressed in the Condition discovered to be inoperable or not within limits, will not result in separate entry into the Condition. Section 1.3 also specifies Required Actions of the Condition continue to apply for each additional failure, with Completion Times based on initial entry into the condition. However, the Required Actions for inoperable RPS manual actuation Functions provide appropriate compensatory measures for separate inoperable Functions. As such, a Note has been provided which allows separate Condition entry for each inoperable RPS manual actuation Function.

BASES

ACTIONS (continued)

A.1

If one manual actuation channel is inoperable the capability to shut down the unit with the associated Function is lost. However, manual shutdown capability is retained by the OPERABLE Function. The 12-hour Completion Time is intended to allow the operator time to evaluate and repair any discovered inoperabilities. The 12-hour Completion Time is acceptable based on engineering judgment considering the availability of the automatic functions and alternative manual trip methods and the low probability of an event requiring manual reactor scram during this interval. The four RPS automatic divisions also have manual trip capability provided by four divisional trip switches that are located in positions easily accessible for optional use by the plant operator.

Alternatively, if it is not desired to place the inoperable channel in trip (e.g., as in the case where placing the inoperable channel in trip would result in a scram), Condition C or D, as appropriate, must be entered and its Required Action taken.

B.1

With one channel of the manual scram Function inoperable and one channel of the Reactor Mode Switch -Shutdown position Function inoperable, the affected channels must be verified in trip immediately. In this Condition, both required manual actuation Functions are inoperable.

Alternatively, if it is not desired to place the inoperable channels in trip (e.g., as in the case where placing the inoperable channels in trip would result in a scram), Condition C or D, as appropriate, must be entered and its Required Action taken.

C.1

With both manual actuation channels inoperable in one or both Functions in MODE 1 or 2 or if any Required Action and associated Completion Time of Condition A or B is not met in MODE 1 or 2, 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 12 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 safety systems.

BASES

ACTIONS (continued)

D.1

With both manual actuation channels inoperable in one or both Functions in MODE 6 or if any Required Action and associated Completion Time of Condition A or B is not met in MODE 6, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must immediately initiate action to fully insert all insertable control rods in core cells containing one or more fuel assemblies. Action must continue until all such control rods are fully inserted. Control rods in core cells containing no fuel assemblies do not affect the reactivity of the core and, therefore, do not have to be inserted.

SURVEILLANCE REQUIREMENTS

SR 3.3.1.3.1

A CHANNEL FUNCTIONAL TEST is performed on each RPS Manual Scram Function channel to ensure that each channel will perform the intended Function. The Frequency of 7 days is based on the reliability of the RPS actuation logic and controls.

SR 3.3.1.3.2

A CHANNEL FUNCTIONAL TEST is performed on the Reactor Mode Switch - Shutdown Position Function to ensure that the Reactor Mode Switch will perform the intended Function. The Frequency of 24 months is based on the need to perform this Surveillance under the conditions that apply during a plant outage and the potential for an unplanned transient if the Surveillance were performed with the reactor at power. Operating experience has shown that these components usually pass the Surveillance when performed at the 24-month Frequency.

REFERENCES

None.

B 3.3 INSTRUMENTATION

B 3.3.1.4 Neutron Monitoring System (NMS) Instrumentation

BASES

BACKGROUND

The NMS Instrumentation provides input to the Reactor Protection System (RPS) when sufficient instrumentation channels indicate a trip condition. The RPS is designed to initiate a reactor scram when one or more monitored parameters exceed their specified limit, to preserve the integrity of the fuel cladding and the Reactor Coolant System (RCS), and minimize the energy that must be absorbed following a loss of coolant accident (LOCA).

The protection and monitoring functions of the NMS have been designed to ensure safe operation of the reactor. This is achieved by specifying limiting safety system settings (LSSS) in terms of parameters directly monitored by the RPS, as well as LCOs on other reactor system parameters and equipment performance. Technical Specifications are required by 10 CFR 50.36 to contain LSSS defined by the regulation as "...settings for automatic protective devices related to those variables having significant safety functions." Where LSSS is specified for a variable on which a Safety Limit (SL) has been placed, the setting must be chosen such that automatic protective action will correct the abnormal situation before a SL is exceeded. The Analytical Limit is the limit of the process variable at which a safety action is initiated, as established by the safety analysis, to ensure that a SL is not exceeded. Any automatic protection action that occurs on reaching the Analytical Limit therefore ensures that the SL is not exceeded. Where LSSS is specified for a variable having a significant safety function but which does not protect the SLs, the setting must be chosen such that automatic protective actions will initiate consistent with the design basis. The Design Limit is the limit of the process variable at which a safety function is initiated to ensure that these automatic protective devices will perform their specified safety function.

The actual settings for automatic protective devices must be chosen to be more conservative than the Analytical / Design Limit to account for instrument loop uncertainties related to the setting at which the automatic protective action would actually occur. The methodology for determining the actual settings, and the required tolerances to maintain these settings conservative to the Analytical / Design Limits, including the requirements for determining that the channel is OPERABLE, are defined in the Setpoint Control Program (SCP), in accordance with Specification 5.5.11, "Setpoint Control Program (SCP)."

BASES

BACKGROUND (continued)

The Limiting Trip Setpoint (LTSP) is a predetermined setting for a protective device chosen to ensure automatic actuation prior to the process variable reaching the Analytical / Design Limit and thus ensuring that the SL would not be exceeded (i.e., for Analytical Limits), or that automatic protective actions occur consistent with the design basis (i.e., for Design Limits). As such, the LTSP accounts for process and primary element measurement errors, and uncertainties in setting the device (e.g., calibration), uncertainties in how the device might actually perform (e.g., accuracy), changes in the point of action of the device over time (e.g., drift during surveillance intervals), and any other factors, which may influence its actual performance (e.g., harsh accident environments). In this manner, the LTSP ensures that SLs are not exceeded and that automatic protective devices will perform their specified safety function. As such, the LTSP meets the definition of an LSSS. The nominal trip setpoint to which the setpoint is reset after calibration is the $NTSP_F$, which is more conservative than the LTSP and has margin to assure that the Allowable Value is not exceeded during calibration.

Technical Specifications contain values related to the OPERABILITY of equipment required for safe operation of the facility. OPERABLE is defined in Technical Specifications as "...being capable of performing its safety function(s)." For automatic protective devices, the required safety function is to ensure that a SL is not exceeded and that automatic protective actions will initiate consistent with the design basis. Therefore, the LTSP is the LSSS as defined by 10 CFR 50.36. However, use of the LTSP to define OPERABILITY in Technical Specifications would be an overly restrictive requirement if it were applied as an OPERABILITY limit for the "as found" value of a protective device setting during a Surveillance.

However, there is also some point beyond which the device would have not been able to perform its function due, for example, to greater than expected drift. This value is specified in the SCP, as required by Specification 5.5.11, in order to define OPERABILITY of the devices and is designated as the Allowable Value which is the least conservative value of the as-found setpoint that a channel can have during CHANNEL CALIBRATION. The LTSP, $NTSP_F$, Allowable Value, "as-found" tolerance, and "as-left" tolerance, and the methodology for calculating the ALT and AFT will be maintained in the SCP, as required by Specification 5.5.11.

BASES

BACKGROUND (continued)

The Allowable Value is the least conservative value that the setpoint of the channel can have when tested such that a channel is OPERABLE if the setpoint is found conservative with respect to the Allowable Value during the CHANNEL CALIBRATION. Note that, although a channel is OPERABLE under these circumstances, the setpoint must be left adjusted to a value within the established "as-left" tolerance of the $NTSP_F$ and confirmed to be operating within the statistical allowances of the uncertainty terms assigned in the setpoint calculation. As such, the Allowable Value differs from the $NTSP_F$ by an amount equal to or greater than the "as-found" tolerance value. In this manner, the actual setting of the device will ensure that a SL is not exceeded or that automatic protective actions will initiate consistent with the design basis at any given point of time as long as the device has not drifted beyond that expected during the surveillance interval. If the actual setting of the device is found to be non-conservative with respect to the Allowable Value the device would be considered inoperable from a Technical Specification perspective. This requires corrective action including those actions required by 10 CFR 50.36 when automatic protective devices do not function as required.

The NMS is composed of the startup range neutron monitor (SRNM) and the average power range monitor (APRM). SRNM trip signals and APRM trip signals from each of the four divisions of NMS equipment are provided to the four divisions of RPS trip logic (Ref. 1).

The SRNM provides trip signals to the RPS to cover the range of plant operation from source range through startup range (i.e., more than 10% of reactor rated power). Three SRNM conditions, monitored as a function of the NMS, comprise the SRNM trip logic output to the RPS. These conditions are as follows: SRNM Neutron Flux High (high count rate when selected to the non-coincident mode); Neutron Flux Short (fast) Period; and SRNM inoperative. The SRNM Neutron Flux High (non-coincident mode) is not required in any accident analysis in Reference 2. Therefore, OPERABILITY of the SRNM Neutron Flux High (non-coincident mode) is not required by Technical Specifications and is addressed in plant procedures. The trip conditions from every SRNM associated with the same NMS division are combined into a single SRNM trip signal for that division. The specific condition that causes the SRNM trip output state is identified by the NMS and is not detectable within the RPS.

BASES

BACKGROUND (continued)

The SRNM consists of twelve fixed in-core regenerative fission chamber sensors, each with associated electronics to monitor the whole startup range (10 decades) of neutron flux. The twelve detectors are all located at fixed elevation slightly above the mid-plane of the fuel region, and are evenly distributed throughout the core. The twelve SRNM channels are divided into four NMS divisions. For each division, any one SRNM channel trip will result in an SRNM division trip. Each SRNM divisional output is provided to each of the four divisions two-out-of-four voters (NMS Trip Logic Unit). The NMS Trip Logic Unit determines whether there are sufficient SRNM divisions in trip (two-out-of-four logic). In addition, the twelve SRNM channels are divided into four bypass groups. There is one bypass group for each quadrant of the core, consisting of the three SRNMs located in that quadrant. A joystick type bypass switch ensures that no more than one SRNM in a quadrant can be simultaneously bypassed. Thus, up to four channels may be bypassed at any one time. There is no additional SRNM bypass capability at the divisional level; however, it is possible to bypass all three SRNMs within a division.

Each SRNM cabinet is redundantly powered by two uninterruptible divisional 120 VAC power sources from its associated electrical division; either source of power can support system operation.

The APRMs provide trip signals to the RPS to cover the range of plant operation from a few percent to greater than rated power. Three APRM conditions, monitored as a function of the NMS, comprise the APRM trip logic output to the RPS. These conditions are APRM Fixed Neutron Flux -High, Simulated Thermal Power - High, and APRM inoperative.

There are four APRM channels divided into four NMS divisions. For each division, any one APRM channel trip (high or inoperative) will result in a division trip. Each APRM divisional output is provided to each of the four divisions two-out-of-four voters (NMS Trip Logic Unit). The NMS Trip Logic Unit determines whether there are sufficient APRM divisions in trip (two-out-of-four logic). One APRM channel may be bypassed at any one time. When an APRM is bypassed, its associated Oscillation Power Range Monitor (OPRM) is also bypassed.

APRM channels receive power from its associated electrical division. Either of the two redundant uninterruptible power sources within a division can support APRM channel operation.

BASES

BACKGROUND (continued)

The OPRMs provide trip signals to the RPS to cover the range of plant operation from a few percent to greater than rated power. The OPRM trip protection includes algorithms that detect thermal hydraulic instability (flux oscillation with unacceptable amplitude and frequency).

There are four OPRM channels divided into four NMS divisions. The OPRM function resides in its associated APRM channel equipment. For each division, any one OPRM channel trip will result in a division trip.

Each OPRM divisional output is provided to each of the four divisions two-out-of-four voters (NMS Trip Logic Unit). The NMS Trip Logic Unit determines whether there are sufficient OPRM divisions in trip (two-out-of-four logic). When an APRM is bypassed, its associated OPRM is also bypassed. The OPRM function resides in the APRM equipment and receives the same redundant APRM power.

The APRMs, OPRMs, and the SRNM are part of the NMS instrumentation. The trip decisions are made within the NMS. This is done on a divisional basis and the results then sent directly to the RPS Trip Logic Units (TLUs). Thus, each NMS division sends only two inputs to the RPS divisional TLUs, one for APRM trip/no-trip (which includes the OPRM trip) and one for SRNM trip/no-trip. A divisional APRM (OPRM) or SRNM may be tripped due to any of the monitored variables exceeding its trip setpoint. The RPS two-out-of-four trip decision is then made, not on a per variable basis, but on an APRM (OPRM) tripped or SRNM tripped basis, by looking at the four divisions of APRM (OPRM) and four divisions of SRNM. All bypasses of the SRNMs and APRMs (OPRMs) are performed within and by the NMS.

The NMS is designed to provide reliable single-failure proof capability to automatically provide a trip signal to the RPS while maintaining protection against unnecessary trip signals resulting from single failures. The NMS satisfies the single-failure criterion even when one entire division of instrumentation is bypassed and/or when one of the four automatic actuation divisions is out of service.

This Specification addresses OPERABILITY of the SRNM channels from the sensors to the NMS Digital Trip Modules (DTMs) and up to each of the SRNM Trip Logic Units. This Specification addresses OPERABILITY of the APRM and OPRM channels from the sensors (local power range monitors, LPRMs) to the NMS Digital Trip Modules and up to each of the

BASES

BACKGROUND (continued)

NMS Trip Logic Units, which house the APRM/OPRM logic. LCO 3.3.1.5, "Neutron Monitoring System (NMS) Automatic Actuation," addresses OPERABILITY requirements for NMS automatic actuation for the SRNM and the APRM/OPRM.

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

The actions of the NMS in conjunction with RPS are assumed in the safety analyses of References 2 and 3. The NMS provides a trip signal to RPS when monitored parameter values exceed predetermined values specified in the SCP to preserve the integrity of the fuel cladding, preserve the integrity of the reactor coolant pressure boundary, and preserve the integrity of the containment by minimizing the energy that must be absorbed following a LOCA.

NMS Instrumentation satisfies the requirements of Selection Criterion 3 of 10 CFR 50.36(c)(2)(ii). Functions not specifically credited in the accident analysis are retained for the overall redundancy and diversity of the NMS and RPS as required by the NRC approved licensing basis.

The OPERABILITY of the NMS and RPS is dependent on the OPERABILITY of the individual instrumentation channel Functions specified in Table 3.3.1.4-1. Each Function must have the required number of OPERABLE channels, with their setpoints in accordance with the SCP, where appropriate. The actual setpoint is calibrated consistent with the SCP. Each channel must also respond within its assumed response time.

$NTSP_F$s are specified in the SCP, as required by Specification 5.5.11. The $NTSP_F$s are selected to ensure the actual setpoints are conservative with respect to the Allowable Value between successive CHANNEL CALIBRATIONS. Operation with a trip setpoint less conservative than the $NTSP_F$, but conservative with respect to its Allowable Value, is acceptable. A channel is inoperable if its actual trip setpoint is non-conservative with respect to its required Allowable Value.

The individual Functions are required to be OPERABLE in the MODES specified in the Table which may require an RPS trip to mitigate the consequences of a design basis accident or transient. To ensure a reliable scram function, a combination of Functions is required in each MODE.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

Although there are four divisions of NMS instrumentation for each function, only three divisions of NMS instrumentation for each function are required to be OPERABLE. The three required divisions are those divisions associated with the DC and Uninterruptible AC Electrical Power Distribution Divisions required by LCO 3.8.6, "Distribution Systems - Operating," and LCO 3.8.7, "Distribution Systems - Shutdown." This is acceptable because the single-failure criterion is met with three OPERABLE NMS instrumentation divisions, and because each NMS division is associated with and receives power from only one of the four electrical divisions.

The specific Applicable Safety Analyses, LCO and Applicability discussions are listed below on a Function-by-Function basis.

1.a. Startup Range Neutron Monitor (SRNM) Neutron Flux - Short Period

The SRNM subsystem is part of the NMS. The SRNMs monitor neutron flux levels from cold shutdown condition to high neutron flux range with the LPRM/APRM on scale and with sufficient overlap of flux indication between the SRNMs and the APRMs. The SRNMs monitor the power level over the range from source range to more than 10% RTP. The SRNM subsystem will generate a scram trip signal to prevent fuel damage in the event of any abnormal positive reactivity insertion transients while operating in the startup power range. This trip signal is to be generated for an excessive neutron flux increase rate, i.e., short reactor period. The setpoint of this trip is determined such that under the worst positive reactivity insertion event, fuel integrity is always protected. The worst bypass or out of service condition of the SRNM subsystem is considered in determining the setpoints. In the startup power range, the most significant source of positive reactivity change is due to control rod withdrawal. The SRNM provides diverse protection for the Rod Worth Minimizer (RWM) in the Rod Control and Information System (RC&IS), which monitors and controls the movement of control rods at low power. The RWM prevents the withdrawal of an out of sequence control rod during startup that could result in an unacceptable neutron flux excursion (Ref. 4). The SRNM provides mitigation of the neutron flux excursion.

The SRNMs are also capable of limiting other reactivity excursions during startup such as cold-water injection events although no credit is specifically assumed.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

The SRNM consists of twelve fixed in-core regenerative fission chamber sensors, each with associated electronics to monitor the whole startup range (10 decades) of neutron flux. The twelve detectors are all located at fixed elevation about the mid-plane of the fuel region, and are evenly distributed throughout the core. The twelve SRNM channels are divided into four NMS divisions. For each division, any one SRNM channel trip will result in an SRNM division trip. Therefore, two SRNM instrument channels are required to be OPERABLE in each required NMS division. Each SRNM divisional output is provided to each of the four divisions (NMS Trip Logic Unit). The NMS Trip Logic Unit determines whether there are sufficient SRNM divisions in trip (two-out-of-four logic). In addition, the twelve SRNM channels are divided into four bypass groups. There is one bypass group for each quadrant of the core, consisting of the three SRNMs located in that quadrant. A joystick type bypass switch ensures that no more than one SRNM in a quadrant can be simultaneously bypassed. Thus, up to four channels may be bypassed at any one time. There is no additional SRNM bypass capability at the divisional level; however, it is possible to bypass all of the SRNMs within a division.

Three divisional channels of each SRNM Function, with two separate channels per division, are required to be OPERABLE to ensure no single instrument failure will preclude a scram from these Functions on a valid signal.

The Allowable Value for the Startup Range Neutron Monitor (SRNM) Neutron Flux - Short Period Function is set to mitigate the consequences of a rod withdrawal error.

The SRNM Neutron Flux - Short Period Function must be OPERABLE during MODE 2 when control rods may be withdrawn and the potential for criticality exists. In MODE 1, the Average Power Range Monitor Fixed Neutron Flux - High Function and the Automated Thermal Limit Monitor (ATLM) provides protection against reactivity transients. The SRNM Neutron Flux – Short Period Function is required to be OPERABLE in MODE 6 with any control rod withdrawn from a core cell containing one or more fuel assemblies. During normal operation in MODES 3, 4, and 5, all control rods are fully inserted and the Reactor Mode Switch - Shutdown Position control rod withdrawal block (LCO 3.3.2.1, "Control Rod Block Instrumentation") does not allow any control rod to be withdrawn. Control rods withdrawn from a core cell containing no fuel assemblies do not

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

affect the reactivity of the core and therefore are not required to have the capability to scram. Provided all control rods otherwise remain inserted, the SRNM function is not required. In this condition the required SDM (LCO 3.1.1, "SHUTDOWN MARGIN") and refuel position one-rod /rod-pair-out interlock (LCO 3.9.2, "Refuel Position One-Rod/Rod-Pair-Out Interlock") ensures no event requiring RPS will occur. Under these conditions, the SRNM Function is not required to be OPERABLE.

1.b. SRNM - Inop

This trip signal provides assurance that a minimum number of SRNMs are OPERABLE. Anytime a SRNM detector high voltage drops below a preset level or when a module is disconnected an inoperative trip signal will occur unless the SRNM is bypassed.

This Function was not specifically credited in the accident analysis but it is retained for the overall redundancy and diversity of the RPS as required by the NRC approved licensing basis.

Three divisional channels of the SRNM Inop Function, with two separate channels per division, are required to be OPERABLE to ensure no single instrument failure will preclude a scram from these Functions on a valid signal.

This Function is required to be OPERABLE when the SRNM Neutron Flux - Short Period Function is required.

2.a. APRM Fixed Neutron Flux - High, Setdown

The APRM channels receive input signals from the LPRMs within the reactor core to provide an indication of the power distribution and local power changes. The APRM channels average these LPRM signals to provide a continuous indication of average reactor power from a few percent to greater than RATED THERMAL POWER. For operation at low power (i.e., MODE 2), the APRM Fixed Neutron Flux - High Setdown Function is capable of generating a trip signal that prevents fuel damage resulting from abnormal operating transients in this power range. For most operation at low power levels, the APRM Fixed Neutron Flux - High, Setdown Function will provide a secondary scram to the SRNM Neutron Flux - High Function because of the relative setpoints. With the SRNM near its high power range, it is possible that the APRM Fixed Neutron

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

Flux - High, Setdown Function will provide the primary trip signal for a core wide increase in power.

The control rod withdrawal event during startup (Ref. 4) assumes the failure of the SRNM instrumentation and shows that the APRM Fixed Neutron Flux - High, Setdown Function is capable of maintaining the peak fuel enthalpy to within limits so that no fuel damage results. However, this Function indirectly ensures that before the reactor mode switch is placed in the run position, reactor power does not exceed 25% RTP (Safety Limit 2.1.1.1) when operating at low reactor pressure and low core flow. It therefore indirectly prevents fuel damage during significant reactivity increases with THERMAL POWER < 25% RTP.

Three channels of APRM Fixed Neutron Flux - High, Setdown are required to be OPERABLE to ensure no single failure will preclude a scram from this Function on a valid signal. In addition, sufficient LPRM inputs are required to be OPERABLE to provide adequate coverage of the entire core.

The Allowable Value is based on preventing significant increases in power when THERMAL POWER is < 25% RTP.

The APRM Fixed Neutron Flux - High, Setdown Function must be OPERABLE during MODE 2 when control rods may be withdrawn. In MODE 1, the Average Power Range Monitor Fixed Neutron Flux - High Function and the ATLM provides protection against reactivity transients.

2.b. APRM Simulated Thermal Power - High

The APRM Simulated Thermal Power - High Function monitors neutron flux to approximate the thermal power being transferred to the reactor coolant. The APRM simulated thermal power signal represents the APRM flux signal through a time constant representing the actual fuel time constant. The simulated thermal power signal accurately represents core thermal (as opposed to neutron flux) power and the heat flux through the fuel. The signal is fixed at an upper limit that is always lower than the APRM Fixed Neutron Flux - High Function Setpoint. The APRM

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

Simulated Thermal Power - High Function provides protection against transients where thermal power increases slowly (such as the Loss of Feedwater Heating event) however this Function is not credited. During these events, the thermal power increase does not significantly lag the neutron flux response and, because of a lower trip setpoint, will initiate a scram before the high neutron flux scram. For rapid neutron flux increase events, the thermal power lags the neutron flux and the APRM Fixed Neutron Flux - High Function will provide a scram signal before the APRM Simulated Thermal Power - High Function setpoint is exceeded.

Three channels of APRM Simulated Thermal Power - High Function are required to be OPERABLE to ensure no single failure will preclude a scram from this Function on a valid signal.

The Allowable Value for the APRM Simulated Thermal Power - High Function is based on the mitigation of the Loss of Feedwater Heater event, however no credit is taken for this Function.

The thermal power time constant of less than seven seconds is based on the fuel heat transfer dynamics and provides a signal proportional to the thermal power.

The APRM Simulated Thermal Power - High Function is required to be OPERABLE in MODE 1 when there is the possibility of generating excessive thermal power and potentially exceeding the Safety Limit applicable to high pressure and core flow conditions (fuel cladding integrity Safety Limit). During MODES 2 and 6, other SRNM and APRM Functions provide protection for fuel cladding integrity.

<u>2.c. APRM Fixed Neutron Flux - High</u>

The APRM channels provide the primary indication of neutron flux within the core and respond almost instantaneously to neutron flux increases. For the overpressurization protection analysis of Reference 3, the APRM Fixed Neutron Flux - High Function is assumed to terminate the MSIV Closure event and, along with the safety relief valves, limits the peak Reactor Pressure Vessel (RPV) pressure to less than the ASME Code limits. This Function is also credited in the pressure regulator failure event (Ref. 5)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

Three channels of APRM Fixed Neutron Flux - High Function are required to be OPERABLE to ensure no single failure will preclude a scram from this Function on a valid signal. In addition, sufficient LPRM inputs are required to be OPERABLE to provide adequate coverage of the entire core.

The Allowable Value is based on the overpressurization and pressure regulator failure event.

The APRM Fixed Neutron Flux - High Function is required to be OPERABLE in MODE 1 where the potential consequences of the analyzed transients could result in the Safety Limit (e.g., Reactor Vessel pressure) being exceeded. In MODE 2, the APRM Fixed Neutron Flux - High, Setdown Function and the SRNM trips provide adequate protection. Therefore, the APRM Fixed Neutron Flux - High Function is not required in MODE 2.

2.d. APRM - Inop

This signal provides assurance that a minimum number of APRMs are OPERABLE. Anytime a failure occurs that causes a channel to become inoperative or the APRM has too few LPRM inputs, an inoperative trip signal is automatically generated by that APRM channel, unless the APRM is bypassed.

This Function was not specifically credited in the accident analysis but it is retained for the overall redundancy and diversity of the RPS as required by the NRC approved licensing basis.

Three channels of APRM - Inop are required to be OPERABLE to ensure no single failure will preclude a scram from this Function on a valid signal.

There is no Allowable Value for this Function.

This Function is required to be OPERABLE in the MODES where the APRM Functions are required.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

3. Oscillation Power Range Monitor - Upscale

The Oscillation Power Range Monitor (OPRM) consists of four channels. The OPRM channel utilizes the same set of LPRM signals used by the associated APRM channel in which this OPRM channel resides and forms many OPRM cells to monitor the neutron flux behavior of all regions of the core. The LPRM signals assigned to each cell are summed and averaged to provide an OPRM signal for this cell. The OPRM trip protection algorithms detect thermal hydraulic instability (flux oscillation with unacceptable amplitude and frequency) and provide trip output to the RPS if the trip setpoint is exceeded.

Three channels of OPRM are required to be OPERABLE to ensure no single failure will preclude a scram from this Function on a valid signal. In addition, sufficient LPRM inputs are required to be OPERABLE to provide adequate coverage of the entire core .

There is no Allowable Value for this Function. The OPRM trip setpoints are established in accordance with the methodologies defined in Reference 6, and are documented in the Core Operating Limits Report (COLR).

The OPRM – Upscale Function is not credited in the safety analysis and is included in the Technical Specifications as a defense-in-depth feature. The OPRM – Upscale Function is provided as a backup to other RPS Functions and the Selected Control Rod Run-In/ Select Rod Insert (SCRRI/SRI) function. The OPRM Function is required to be OPERABLE when THERMAL POWER is ≥ 25% RTP. The OPRM – Upscale Function is automatically enabled (bypass removed) when THERMAL POWER is ≥ 25% RTP.

ACTIONS

A Note has been provided to modify the ACTIONS related to NMS Instrumentation channels. Section 1.3, Completion Times, specifies once a Condition has been entered, subsequent divisions, subsystems, components or variables expressed in the Condition discovered to be inoperable or not within limits, will not result in separate entry into the Condition. Section 1.3 also specifies Required Actions of the Condition continue to apply for each additional failure, with Completion Times based on initial entry into the condition. However, the Required Actions for inoperable NMS Instrumentation channels provide appropriate

BASES

ACTIONS (continued)

compensatory measures for separate inoperable channels. As such, a Note has been provided which allows separate Condition entry for each inoperable NMS Instrumentation channel.

A.1

The 12-hour Completion Time is acceptable based on engineering judgment considering the diversity of trip signals available, the redundancy of the NMS and RPS design, and the low probability of an event requiring a reactor scram during this interval. However, this out of service time is only acceptable provided the associated Function still maintains NMS actuation capability (refer to Required Action B.1 Bases). If the inoperable channel cannot be restored to OPERABLE status within the 12-hour Completion Time, the associated NMS instrument channel must be verified to be in trip. Verifying the affected NMS instrument channel in trip conservatively compensates for the inoperability and allows operation to continue.

Alternatively, if it is not desirable to verify the associated instrument channel in trip, Condition C must be entered and its Required Action taken when the Completion Time of Required Action A.1 expires.

B.1

Required Action B.1 directs entry into the appropriate Condition referenced in Table 3.3.1.4-1 if the Required Action and Completion Time of Condition A is not met or if multiple, inoperable, untripped channels for the same Function result in the Function not maintaining NMS trip capability. A Function is considered to be maintaining NMS trip capability when sufficient required channels are OPERABLE or in trip (or the associated NMS division is in trip), such that two divisions will generate a trip signal from the given Function on a valid signal. For the SRNM Functions, this would require two SRNM divisions to have one channel OPERABLE or tripped (or the associated SRNM division in trip). For the APRM Functions, this would require two APRM/OPRM divisions to have one channel OPERABLE or in trip (or the associated APRM/OPRM division in trip). The applicable Condition specified in the Table is Function and MODE or other specified condition dependent and may change as the Required Action of a previous Condition is completed.

BASES

ACTIONS (continued)

C.1 and D.1

If a channel is not restored to OPERABLE status or is not in trip as required within the allowed Completion Time, or if NMS trip capability is not maintained, the plant must be placed in a MODE or other specified condition in which the LCO does not apply. The allowed Completion Times are reasonable, based on operating experience, to reach the specified condition from full power conditions in an orderly manner and without challenging plant systems.

E.1 and E.2

If the channel(s) is not restored to OPERABLE status or is not in trip within the allowed Completion Time, or if NMS trip capability is not maintained, an alternate method to detect and suppress thermal hydraulic instability oscillations (Ref. 7) must be initiated within 12 hours and the inoperable channel(s) must be restored to OPERABLE status within 120 days.

The alternate methods would adequately address detection and mitigation in the event of thermal hydraulic instability oscillations. Based on industry operating experience with actual instability oscillations, the operator would be able to recognize instabilities during this time and take action to suppress them through a manual scram. In addition, the OPRM system may still be available to provide alarms to the operator if the onset of oscillations were to occur.

The 12-hour Completion Time for Required Action E.1 is based on engineering judgment, considering the small probability of an instability event occurring during this interval, to allow orderly transition to the alternate methods while limiting the period of time during which no automatic or alternate detect and suppress trip capability is formally in place.

The 120-day Completion Time, is considered adequate based on engineering judgment considering that with operation minimized in regions where oscillations may occur and implementation of the alternate methods, the likelihood of an instability event that could not be adequately handled by the alternate methods during this 120-day period was negligibly small.

BASES

ACTIONS (continued)

F.1

If the channel(s) is not restored to OPERABLE status or the associated instrument channel is not in trip as required within the allowed Completion Time, or if NMS trip capability is not restored within the allowed Completion Time, the plant must be placed in a MODE or other specified condition in which the LCO does not apply. The Completion Times are reasonable, based on operating experience, to reach the specified condition from full power conditions in an orderly manner and without challenging plant systems.

G.1

If the channel(s) is not restored to OPERABLE status or is not in trip as required within the allowed Completion Time, or if NMS trip capability is not maintained, the plant must be placed in a MODE or other specified condition in which the LCO does not apply. This is done by immediately initiating action to fully insert all insertable control rods in core cells containing one or more fuel assemblies. Control rods in core cells containing no fuel assemblies do not affect the reactivity of the core and are, therefore, not required to be inserted. Action must continue until all insertable control rods in core cells containing one or more fuel assemblies are fully inserted.

SURVEILLANCE REQUIREMENTS

As noted at the beginning of the Surveillance Requirements, the SRs for each NMS instrumentation Function are located in the SRs column of Table 3.3.4.1-1.

SR 3.3.1.4.1

Performance of the CHANNEL CHECK once every 12 hours ensures that a gross failure of instrumentation has not occurred.

The NMS is cyclically tested from the sensor input point to the logic contact output by online self-diagnostics. The self-diagnostic capabilities include microprocessor checks, system initialization, watchdog timers, memory integrity checks, input/output (I/O) data integrity checks, communication bus interface checks, and checks on the application program (checksum).

BASES

SURVEILLANCE REQUIREMENTS (continued)

A 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 based on a combination of the channel instrument uncertainties, including indication, and readability. If a channel is outside the match criteria, it may be an indication that the instrument has drifted outside its limit.

The Surveillance Frequency is based upon operating experience that demonstrates channel failure is rare. The CHANNEL CHECKS every 12 hours supplement less formal, but more frequent checks of channels during normal operational use of the displays associated with the channels required by the LCO.

<u>SR 3.3.1.4.2</u>

To ensure the APRMs are accurately indicating the true core average power, the APRMs are calibrated to the reactor power calculated from a heat balance. The Frequency of once per 7 days is based on minor changes in LPRM sensitivity, which could affect the APRM reading between performances of SR 3.3.1.4.5 (LPRM calibrations).

A Note is provided which only requires performance of the SR to be met at ≥ 25% RTP because it is difficult to accurately determine core THERMAL POWER from a heat balance when < 25% RTP. At low power levels, a high degree of accuracy is unnecessary because of the large, inherent margin to thermal limits (MCPR). At ≥ 25% RTP, the surveillance is required to have been satisfactorily performed within the last 7 days in accordance with SR 3.0.2. A Note is provided which allows an increase in THERMAL POWER above 25% if the 7-day Frequency is not met per SR 3.0.2. In this event, the SR must be performed within 12 hours after reaching or exceeding 25% RTP. The 12 hours is based on operating experience and in consideration of providing a reasonable time in which to complete the SR.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.1.4.3

A CHANNEL FUNCTIONAL TEST is performed on each required channel to ensure that the entire channel will perform the intended function when required. This test ensures a complete CHANNEL FUNCTIONAL TEST of required instrument channels from the sensor input through the NMS DTM function.

The NMS is cyclically tested from the sensor input point to the logic contact output by online self-diagnostics. The self-diagnostic capabilities include microprocessor checks, system initialization, watchdog timers, memory integrity checks, input/output (I/O) data integrity checks, communication bus interface checks, and checks on the application program (checksum).

As noted, for Functions 1.a, 1.b, and 2.a, SR 3.3.1.4.3 is not required to be performed when entering MODE 2 from MODE 1 because testing of the MODE 2 required SRNM and APRM Functions cannot be performed in MODE 1. This allows entry into MODE 2 if the 24-month Frequency is not met per SR 3.0.2. In this event, the SR must be performed within 12 hours after entering MODE 2 from MODE 1. Twelve hours is based on operating experience and in consideration of providing a reasonable time in which to complete the SR.

A Surveillance Frequency of 7 days provides an acceptable level of system average unavailability over the Surveillance Frequency interval.

SR 3.3.1.4.4

A CHANNEL FUNCTIONAL TEST is performed on each required channel to ensure that the entire channel will perform the intended function. This test ensures a complete CHANNEL FUNCTIONAL TEST of required instrument channels from the sensor input through the NMS DTM function.

The NMS is cyclically tested from the sensor input point to the logic contact output by online self-diagnostics. The self-diagnostic capabilities include microprocessor checks, system initialization, watchdog timers, memory integrity checks, input/output (I/O) data integrity checks, communication bus interface checks, and checks on the application program (checksum).

BASES

SURVEILLANCE REQUIREMENTS (continued)

The Frequency of 31 days is based on the reliability of the channels.

SR 3.3.1.4.5

LPRM gain settings are determined from the local flux profiles measured by the automatic fixed in-core probe (AFIP) subsystem of NMS. This establishes the relative local flux profile for appropriate representative input to the APRM system. The 750 MWD/T Surveillance Frequency is based on operating experience with LPRM sensitivity changes.

SR 3.3.1.4.6

A CHANNEL CALIBRATION is a complete check of the instrument loop and the sensor. This test verifies that the required channel responds to the measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the required channel adjusted to the $NTSP_F$ within the "as-left" tolerance to account for instrument drifts between successive calibrations consistent with the methods and assumptions required by the SCP.

SR 3.3.1.4.6 is modified by two Notes. Note 1 states, for Functions 1.a, 1.b, and 2.a, SR 3.3.1.4.5 is not required to be performed when entering MODE 2 from MODE 1 because testing of the MODE 2 required SRNM and APRM Functions cannot be performed in MODE 1. This allows entry into MODE 2 if the Frequency is not met per SR 3.0.2. In this event, the SR must be performed within 12 hours after entering MODE 2 from MODE 1. Twelve hours is based on operating experience and in consideration of providing a reasonable time in which to complete the SR. Note 2 states that neutron detectors are excluded from CHANNEL CALIBRATION because of the difficulty of simulating a meaningful signal. Changes in neutron detector sensitivity are compensated for by performing the calorimetric calibration (SR 3.3.1.4.2) and the LPRM calibration (SR 3.3.1.4.5). The Surveillance Frequency of SR 3.3.1.4.6 is based upon the assumption of a 24 month calibration interval in the determination of the magnitude of equipment drift in the setpoint analysis.

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.1.4.7

The APRM Simulated THERMAL POWER - High Function uses time constant to generate a signal proportional to the core THERMAL POWER from the APRM neutron flux signal. This time constant is representative of the fuel heat transfer dynamics that produce the relationship between the neutron flux and the core THERMAL POWER. The time constant must be verified to ensure that the channel is accurately reflecting the desired parameter.

The 24 month Frequency is based on engineering judgment considering the reliability of the components.

SR 3.3.1.4.8

This SR ensures that the individual required channel response times are less than or equal to the maximum values assumed in the accident analysis. The RPS RESPONSE TIME acceptance criteria are included in Reference 8. RPS RESPONSE TIME may be verified by actual response time measurements in any series of sequential, overlapping, or total channel measurements. This test encompasses the SRNM channels from the sensors to the NMS Digital Trip Modules and up to each of the SRNM Trip Logic Units and the APRM and OPRM channels from the sensors (LPRMs) to the NMS Digital Trip Modules and up to each of the NMS Trip Logic Units, which house the APRM/OPRM logic. This test overlaps the testing required by SR 3.3.1.5.2 to ensure complete testing of instrument channels and actuation circuitry.

COL 16.0-1-A 3.3.1.4-2

[However, some sensors are allowed to be excluded from specific RPS RESPONSE TIME measurement if the conditions of Reference XX are satisfied. If these conditions are satisfied, sensor response time may be allocated based on either assumed design sensor response time or the manufacturer's stated design response time. When the requirements of Reference XX are not satisfied, sensor response time must be measured.

Furthermore, measurement of the instrument loops response times for some sensors is not required if the conditions of Reference XX are satisfied.]

As noted, neutron detectors are excluded from RPS RESPONSE TIME testing because the principles of detector operation virtually ensure an instantaneous response time.

BASES

SURVEILLANCE REQUIREMENTS (continued)

RPS RESPONSE TIME tests are conducted on a 24 month STAGGERED TEST BASIS for three channels. The Frequency of 24 months on a STAGGERED TEST BASIS ensures that the channels associated with each required division are alternately tested. The 24 month test Frequency is consistent with the typical refueling cycle and with operating experience that shows that random failures of instrumentation components causing serious response time degradation, but not channel failure, are infrequent.

SR 3.3.1.4.9

This surveillance involves confirming the OPRM - Upscale trip auto-enable setpoints. This surveillance ensures that the OPRM - Upscale trip is enabled (not bypassed) when THERMAL POWER is ≥ 25% RTP.

If any auto-enable setpoint is nonconservative (i.e., the OPRM - Upscale trip is bypassed when THERMAL POWER is ≥ 25% RTP), then the affected channel is considered inoperable for the OPRM - Upscale Function. Alternatively, the OPRM - Upscale trip auto-enable setpoint(s) may be adjusted to place the channel in a conservative condition (not bypassed). If the OPRM - Upscale trip is placed in the not-bypassed condition, this SR is met and the channel is considered OPERABLE.

The Frequency of 24 months is based on engineering judgment and reliability of the components.

REFERENCES

1. Chapter 7, Figure 7.2-1.
2. Chapter 15
3. Subsection 5.2.2.
4. Subsection 15.3.8.
5. Subsection 15.3.4.
6. Subsection 4D.3.2.2.
7. Subsection 4D.3.3
8. Section 15.2.

B 3.3 INSTRUMENTATION

B 3.3.1.5 Neutron Monitoring System (NMS) Automatic Actuation

BASES

BACKGROUND

The NMS Instrumentation provides input to the Reactor Protection System (RPS) when sufficient instrumentation channels indicate a trip condition. The RPS is designed to initiate a reactor scram when one or more monitored parameters exceed their specified limit, to preserve the integrity of the fuel cladding and the Reactor Coolant System (RCS), and minimize the energy that must be absorbed following a loss of coolant accident (LOCA).

A detailed description of the NMS instrumentation and NMS actuation logic is provided in the Bases for LCO 3.3.1.4, “Neutron Monitoring System (NMS) Instrumentation.”

This Specification addresses OPERABILITY of the NMS automatic actuation divisions that include the Startup Range Neutron Monitor (SRNM) Trip Logic Units, the Average Power Range Monitor (APRM) Trip Logic Units, which house the Oscillation Power Range Monitor (OPRM) logic, and the associated output to RPS (LCO 3.3.1.1, "Reactor Protection System (RPS) Instrumentation"). LCO 3.3.1.4, covers SRNM and APRM (OPRM) channel inputs to the NMS Digital Trip Modules.

APPLICABLE SAFETY ANALYSES

The actions of the NMS in conjunction with RPS are assumed in the safety analyses of Reference 1. The NMS provides a trip signal to RPS when monitored parameter values exceed the trip setpoints to preserve the integrity of the fuel cladding, preserve the integrity of the reactor coolant pressure boundary, and preserve the integrity of the containment by minimizing the energy that must be absorbed following a LOCA.

NMS Automatic Actuation satisfies the requirements of Selection Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

Three SRNM automatic actuation divisions and three APRM/OPRM automatic actuation divisions are required to be OPERABLE to ensure no single automatic actuation division failure will preclude a scram to occur on a valid signal. The three required divisions are those divisions associated with the DC and Uninterruptible AC Electrical Power Distribution Divisions required by LCO 3.8.6, "Distribution Systems -

BASES

LCO (continued)

Operating," and LCO 3.8.7, "Distribution Systems - Shutdown." This is acceptable because the single-failure criterion is still met with three OPERABLE NMS actuation divisions, and because each NMS division is associated with and receives power from only one of the four electrical divisions. This Specification addresses OPERABILITY requirements of the NMS actuation circuitry that includes the interface units and the associated output to RPS.

APPLICABILITY

Three SRNM automatic actuation divisions are required to be OPERABLE in MODE 2 and in MODE 6 with any control rod withdrawn from a core cell containing one or more fuel assemblies. In these conditions, the control rods are assumed to function during a DBA or transient and therefore the four SRNM automatic actuation channels are required to be OPERABLE. In MODES 3, 4, and 5, control rods are not able to be withdrawn since the reactor mode switch is in shutdown and a control rod block is applied. Therefore, SRNM automatic actuation is not required to be OPERABLE in these MODES.

Three APRM automatic actuation divisions are required to be OPERABLE in MODES 1 and 2. In these conditions, the control rods are assumed to function during a DBA or transient and therefore the APRM automatic actuation channels are required to be OPERABLE. In MODES 3, 4, and 5, control rods are not able to be withdrawn since the reactor mode switch is in shutdown and a control rod block is applied. Therefore, the APRM automatic actuation channels are not required to be OPERABLE in these MODES. In MODE 6 with any control rod withdrawn from a core cell containing one or more fuel assemblies, the APRM automatic actuation channels are not required to support the APRM instrumentation in LCO 3.3.1.4, therefore APRM automatic actuation channels are not required to be OPERABLE in these MODES.

Three OPRM automatic actuation divisions are required to be OPERABLE when THERMAL POWER is ≥ 25% RTP.

ACTIONS

A Note has been provided to modify the ACTIONS related to NMS automatic actuation divisions. Section 1.3, Completion Times, specifies once a Condition has been entered, subsequent divisions, subsystems, components or variables expressed in the Condition discovered to be inoperable or not within limits, will not result in separate entry into the Condition. Section 1.3 also specifies Required Actions of the Condition

ACTIONS (continued)

continue to apply for each additional failure, with Completion Times based on initial entry into the condition. However, the Required Actions for inoperable NMS automatic actuation divisions provide appropriate compensatory measures for separate inoperable divisions. As such, a Note has been provided which allows separate Condition entry for each inoperable NMS automatic actuation channel.

A.1

The 12 hour Completion Time is acceptable based on engineering judgment considering the diversity of sensors available to provide trip signals, the redundancy of the NMS and RPS design, and the low probability of event requiring a reactor scram during this interval. However, this out of service time is only acceptable provided the associated Function still maintains NMS trip capability (refer to Required Actions B.1 Bases). If the inoperable division cannot be restored to OPERABLE status within the 12-hour Completion Time, the affected actuation division must be verified to be in trip. Verifying the affected NMS actuation division in trip conservatively compensates for the inoperability and allows operation to continue.

Alternatively, if it is not desirable to verify the affected actuation division in trip (as in the case where it is desired to place the affected actuation division in bypass), Condition C must be entered and its Required Action taken when the Completion Time of Required Action A.1 expires.

B.1

Required Action B.1 directs entry into the appropriate Condition referenced in Table 3.3.1.5-1 if the Required Action and associated Completion Time of Condition A is not met or if multiple, inoperable, untripped divisions (i.e., two or more required divisions) for the same Function result in the Function not maintaining NMS trip capability. A Function is considered to be maintaining NMS trip capability when sufficient divisions are OPERABLE or in trip such that the NMS logic will generate a trip signal from the given Function on a valid signal. For the NMS automatic actuation divisions, two divisions must be OPERABLE or in trip to maintain NMS trip capability.

The applicable Condition specified in the Table is Function and MODE or

BASES

ACTIONS (continued)

other specified condition dependent and may change as the Required Action of a previous Condition is completed.

C.1 and C.2

If the channel(s) is not restored to OPERABLE status or is not in trip within the allowed Completion Time, or if NMS trip capability is not maintained, an alternate method to detect and suppress thermal hydraulic instability oscillations (Ref. 2) must be initiated within 12 hours and the inoperable channel(s) must be restored to OPERABLE status within 120 days.

The alternate methods would adequately address detection and mitigation in the event of thermal hydraulic instability oscillations. Based on industry operating experience with actual instability oscillations, the operator would be able to recognize instabilities during this time and take action to suppress them through a manual scram. In addition, the OPRM system may still be available to provide alarms to the operator if the onset of oscillations were to occur.

The 12-hour Completion Time for Required Action C.1 is based on engineering judgment, considering the small probability of an instability event occurring during this interval, to allow orderly transition to the alternate methods while limiting the period of time during which no automatic or alternate detect and suppress trip capability is formally in place.

The 120-day Completion Time for Required Action C.2 is considered adequate based on engineering judgment considering that with operation minimized in regions where oscillations may occur and implementation of the alternate methods, the likelihood of an instability event that could not be adequately handled by the alternate methods during this 120-day period was negligibly small.

D.1

If the channel(s) is not restored to OPERABLE status or the associated division is not in trip as required within the allowed Completion Time, or if NMS trip capability is not restored within the allowed Completion Time, the plant must be placed in a MODE or other specified condition in which the LCO does not apply. The Completion Times are reasonable, based on operating experience, to reach the specified condition from full power conditions in an orderly manner and without challenging plant systems.

BASES

ACTIONS (continued)

E.1 and F.1

If the affected actuation division is not restored to OPERABLE status, or is not in trip, within the allowed Completion Time, or if NMS actuation capability is not maintained, the plant must be placed in a MODE or other specified condition in which the LCO does not apply. The Completion Times are reasonable, based on operating experience, to reach the specified condition from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.3.1.5.1

The LOGIC SYSTEM FUNCTIONAL TEST demonstrates the OPERABILITY of the NMS automatic actuation divisions. The testing in LCO 3.3.1.1, 3.3.1.2, LCO 3.3.1.4, and the functional testing of control rods in LCO 3.1.3, overlaps this Surveillance to provide complete testing of the assumed safety function.

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 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 24-month Frequency.

SR 3.3.1.5.2

This SR ensures that the individual required division response times are less than or equal to the maximum values assumed in the accident analysis. The RPS RESPONSE TIME acceptance criteria are included in Reference 3.

COL 16.0-1-A 3.3.1.5-2

[However, some portions of the NMS actuation circuitry are allowed to be excluded from specific RPS RESPONSE TIME measurement if the conditions of Reference XX are satisfied. Furthermore, measurement of the instrument loops response times is not required if the conditions of Reference XX are satisfied.]

BASES

SURVEILLANCE REQUIREMENTS (continued)

RPS RESPONSE TIME may be verified by actual response time measurements in any series of sequential, overlapping, or total channel measurements. This test encompasses the NMS automatic actuation divisions that include the SRNM Trip Logic Units, the APRM Trip Logic Units, which house the OPRM logic, and the associated output to RPS. This test overlaps the testing required by SR 3.3.1.4.8 to ensure complete testing of instrument channels and actuation circuitry.

RPS RESPONSE TIME tests are conducted on a 24-month STAGGERED TEST BASIS for three divisions. The Frequency of 24 months on a STAGGERED TEST BASIS ensures that each required division is alternately tested. The 24-month test Frequency is consistent with the refueling cycle and with operating experience that shows that random failures of instrumentation components causing serious response time degradation, but not channel failure, are infrequent.

REFERENCES

1. Chapter 15.

2. Subsection 4D.3.3

3. Section 15.2.

B 3.3 INSTRUMENTATION

B 3.3.1.6 Startup Range Neutron Monitor (SRNM) Instrumentation

BASES

BACKGROUND

The SRNMs provide the operator with information relative to the neutron flux level at very low flux levels in the core. As such, the SRNM indication is used by the operator to monitor the approach to criticality and determine when criticality is achieved.

The SRNM subsystem of the Neutron Monitoring System (NMS) consists of four divisions. Each division includes three SRNMs for a total of twelve SRNMs, each having one fixed in-core regenerative fission chamber sensor. The SRNM instrumentation is discussed in detail in LCO 3.3.1.4, Neutron Monitoring System (NMS) Instrumentation." However, this LCO specifies OPERABILITY requirements only for the monitoring and indication functions of the SRNMs.

During refueling, shutdown, and low-power operations, the primary indication of neutron flux levels is provided by the SRNMs. The SRNMs provide monitoring of reactivity changes during fuel or control rod movement and give the control room operator early indication of unexpected subcritical multiplication that could be indicative of an approach to criticality.

APPLICABLE SAFETY ANALYSES

Prevention and mitigation of prompt reactivity excursions during refueling and low-power operation is provided by:

- LCO 3.1.1, “SHUTDOWN MARGIN (SDM);”
- LCO 3.3.1.1, “Reactor Protection System (RPS) Instrumentation;
- LCO 3.3.1.2, "Reactor Protection System (RPS) Actuation;”
- LCO 3.3.1.4, “Neutron Monitoring System (NMS) Instrumentation;"
- LCO 3.3.1.5, “Neutron Monitoring System (NMS) Automatic Actuation;" and
- LCO 3.3.2.1, “Control Rod Block Instrumentation,” and
- LCO 3.9.1, “Refueling Equipment Interlocks.”

The monitoring requirements of the SRNMs in the Specification have no safety function and are not assumed to function during any design basis accident or transient analysis. However, the SRNMs provide the only on

BASES

APPLICABLE SAFETY ANALYSES (continued)

scale monitoring of neutron flux levels during shutdown and refueling. Therefore, they are being retained in Technical Specifications.

LCO

In MODES 3, 4, and 5, with the reactor shut down, two SRNM channels provide redundant monitoring of flux levels in the core.

In MODE 6, during a spiral off-load or reload, an SRNM outside the fueled region will no longer be required to be OPERABLE, since it is not capable of monitoring neutron flux in the fueled region of the core. Thus, CORE ALTERATIONS are allowed in a quadrant with no OPERABLE SRNM in an adjacent quadrant, as provided in Table 3.3.1.6-1, footnote (a), requirement that the bundles being spiral reloaded, loaded or spiral off-loaded are all in a single fueled region containing at least one OPERABLE SRNM, is met. Spiral reloading and off-loading encompasses reloading or off-loading a cell on the edges of a continuous fueled region (the cell can be reloaded or off-loaded in any sequence).

In non-spiral routine operations, two SRNMs are required to be OPERABLE to provide redundant monitoring of reactivity changes occurring in the reactor core. Because of the local nature of reactivity changes during refueling, adequate coverage is provided by requiring one SRNM to be OPERABLE in the quadrant of the reactor core where CORE ALTERATIONS are being performed and the other SRNM is to be OPERABLE in the same or adjacent quadrant. These requirements ensure that the reactivity of the core will be continuously monitored during CORE ALTERATIONS.

For an SRNM channel to be considered OPERABLE, it must be providing neutron flux monitoring indication.

APPLICABILITY

The SRNMs are required to be OPERABLE in MODES 3, 4, 5, and 6, to provide for neutron monitoring. In MODE 2, the SRNMs are required to be OPERABLE in accordance with LCO 3.3.1.4, "Neutron Monitoring System (NMS) Instrumentation." In MODE 1, the APRMs provide adequate monitoring of reactivity changes in the core; therefore, the SRNMs are not required.

BASES

ACTIONS

A.1 and A.2

With one or more required SRNM channels inoperable in MODE 3, 4, or 5, the neutron flux monitoring capability is degraded or it may not exist. The requirement to fully insert all insertable control rods ensures that the reactor will be at its minimum reactivity level while no neutron monitoring capability is available. Placing the reactor mode switch in the shutdown position prevents subsequent control rod withdrawal by maintaining a control rod block. The allowed Completion Time of 1 hour is sufficient to accomplish the Required Action and is acceptable based on engineering judgment considering the low probability of an event requiring the SRNM occurring during this interval.

B.1 and B.2

With one or more required SRNMs inoperable in MODE 6, the capability to detect local reactivity changes in the core during refueling is degraded. CORE ALTERATIONS must be immediately suspended, and action must be immediately initiated to insert all insertable control rods in core cells containing one or more fuel assemblies. Suspending CORE ALTERATIONS prevents the two most probable causes of reactivity changes, fuel loading and control-rod withdrawal, from occurring. Inserting all insertable control rods ensures that the reactor will be at its minimum reactivity, given that fuel is present in the core. Suspension of CORE ALTERATIONS shall not preclude completion of the movement of a component to a safe, conservative position.

Actions (once required to be initiated) to insert control rods must continue until all insertable rods in core cells containing one or more fuel assemblies are inserted and the required SRNMs are restored to OPERABLE status.

SURVEILLANCE REQUIREMENTS

The SRs for each SRNM Applicable MODE or other specified condition are found in the SRs column of Table 3.3.1.6-1.

SR 3.3.1.6.1 and SR 3.3.1.6.3

Performance of the CHANNEL CHECK ensures that a gross failure of instrumentation has not occurred.

The NMS is cyclically tested from the sensor input point to the logic contact output by online self-diagnostics. The self-diagnostic capabilities include microprocessor checks, system initialization, watchdog timers, memory integrity checks, input/output (I/O) data integrity checks,

BASES

SURVEILLANCE REQUIREMENTS (continued)

communication bus interface checks, and checks on the application program (checksum).

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 match criteria, it may be an indication that the instrument has drifted outside its limit.

The Frequency of once every 12 hours for SR 3.3.1.6.1 is based on operating experience that demonstrates channel failure is rare. While in MODES 3, 4, and 5, reactivity changes are not expected; therefore, the 12-hour Frequency is relaxed to 24 hours for SR 3.3.1.6.3. The CHANNEL CHECK supplements less formal, but more frequent checks of channels during normal operational use of the displays associated with the channels required by the LCO.

SR 3.3.1.6.2

To provide adequate coverage of potential reactivity changes in the core, one SRNM is required to be OPERABLE in the quadrant where CORE ALTERATIONS are being performed and the other OPERABLE SRNM must be in an adjacent quadrant. Note 1 states that this SR is required to be met only during CORE ALTERATIONS. It is not required to be met at other times in MODE 6 since core reactivity changes are not occurring. This Surveillance consists of a review of plant logs to ensure that SRNMs required OPERABLE for given CORE ALTERATIONS are in fact OPERABLE. In the event that only one SRNM is required to be OPERABLE per Table 3.3.1.6-1, footnote (a), only the part ‘a’ portion of this SR is required. Note 2 clarifies that the three requirements can be met by the same or different OPERABLE SRNMs. The 12-hour Surveillance Frequency is based upon operating experience and supplements operational controls over refueling activities, which include steps to ensure the SRNMs required by the LCO are in the proper quadrant.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.1.6.4

This Surveillance consists of a verification of the plant SRNM instrument readout to ensure that the SRNM reading is greater than a specified minimum count rate. This ensures that the detectors are indicating count rates indicative of neutron flux levels within the core. With few fuel assemblies loaded, the SRNMs will not have a high enough count rate to satisfy the Surveillance Requirement. Therefore allowances are made for loading sufficient “source” material, in the form of irradiated fuel assemblies, to establish the minimum count rate.

To accomplish this, the SR is modified by a Note which states that the count rate is not required to be met on an SRNM that has less than or equal to four fuel assemblies adjacent to the SRNM and no other fuel assemblies are in the associated core quadrant. With four or less fuel assemblies loaded around each SRNM and no other fuel assemblies in the associated quadrant, even with a control rod withdrawn, the configuration will not be critical.

The Frequency is based upon channel redundancy and other information available in the control room and ensures the required channels are frequently monitored while core reactivity changes are occurring. When no reactivity changes are in progress, the Frequency is relaxed from 12 hours to 24 hours.

SR 3.3.1.6.5 and SR 3.3.1.6.6

Performance of a CHANNEL FUNCTIONAL TEST demonstrates that the associated channel will function properly.

The NMS is cyclically tested from the sensor input point to the logic contact output by online self-diagnostics. The self-diagnostic capabilities include microprocessor checks, system initialization, watchdog timers, memory integrity checks, input/output (I/O) data integrity checks, communication bus interface checks, and checks on the application program (checksum).

SR 3.3.1.6.5 is required in MODE 6. The 7-day Frequency ensures that the channels are OPERABLE while core reactivity changes could be in progress. The 7-day Frequency is based on operating experience and on other Surveillances (such as CHANNEL CHECK) that ensure proper functioning between CHANNEL FUNCTIONAL TESTS.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.1.6.6 is required in MODES 3, 4, and 5. The Frequency for CHANNEL FUNCTIONAL TESTS has been extended from 7 days to 31 days because core reactivity changes do not normally take place in MODES 3, 4, and 5. The 31-day Frequency is based on operating experience and on other Surveillances (such as CHANNEL CHECK) that ensure proper functioning between CHANNEL FUNCTIONAL TESTS.

SR 3.3.1.6.7

Performance of a CHANNEL CALIBRATION verifies the performance of the SRNM detectors and associated circuitry. The 24-month Frequency considers the unit conditions required to perform the test, the ease of performing the test, the likelihood of a change in the system or component status. The neutron detectors may be excluded from the CHANNEL CALIBRATION because they cannot readily be adjusted. The detectors are regenerative fission chambers that are designed to have a relatively constant sensitivity over the range, and with an accuracy specified for a fixed useful life.

REFERENCES None.

B 3.3 INSTRUMENTATION

B 3.3.2.1 Control Rod Block Instrumentation

BASES

BACKGROUND

Control rods provide the primary means for control of reactivity changes. Control rod block instrumentation includes channel sensors, software, hardware, switches, and relays that are designed to ensure that specified fuel design limits are not exceeded for postulated transients and accidents. During high power operation, the Automated Thermal Limit Monitor (ATLM) provides protection for control rod withdrawal error events. During high power operation, the Multi-Channel Rod Block Monitor (MRBM) provides protection for control rod withdrawal error events, assuming multiple failures of the ATLM. During low power operations, control rod blocks from the Rod Worth Minimizer (RWM) enforce specific control rod sequences designed to limit the consequences of a control rod withdrawal error (RWE). During shutdown conditions, control rod block from the Reactor Mode Switch - Shutdown Position ensures that all control rods remain inserted to prevent inadvertent criticalities.

The purpose of the ATLM is to limit control rod withdrawal if localized neutron flux exceeds a calculated setpoint during control rod manipulations. It is assumed to function to block further control rod withdrawal to preclude a violation of the operating limit MINIMUM CRITICAL POWER RATIO (OLMCPR), the Safety Limit MCPR (SLMCPR), and operating limit MAXIMUM LINEAR HEAT GENERATION RATE (OLMLHGR). The ATLM supplies a trip signal to the Rod Action and Position Information (RAPI) subsystem of Rod Control and Information System (RC&IS) to appropriately inhibit control rod withdrawal during power operations above the ATLM enable setpoint. There are two ATLM channels, either of which can initiate a control rod block when local neutron flux exceeds the ATLM calculated control rod block setpoint. The rod block logic circuitry in the RC&IS is arranged as two redundant and separate logic circuits. Control rod withdrawal is permitted only when the two channels agree, unless one of the channels of logic has been manually bypassed. Control rod position, Local Power Range Monitor (LPRM), and Average Power Range Monitor (APRM) data are the primary data input for the ATLM. APRM signals are used to determine when THERMAL POWER is greater than or equal to the ATLM enable setpoint to enable the ATLM rod block function (Ref. 1).

The ATLM also provides a feedwater temperature control valve one-way block and a rod withdrawal block if the reactor thermal power versus

BASES

BACKGROUND (continued)

feedwater temperature combination is outside of the area allowed by the reactor power versus feedwater temperature map, or if the feedwater temperature decrease causes thermal limit violations. The ATLM provides a feedwater temperature valve one-way block and rod withdrawal block, if the feedwater temperature decreases by more than a set value from a reference feedwater temperature. The safety analyses do not credit the feedwater temperature-related blocks (Refs. 2 and 3); therefore, the feedwater temperature-related blocks of the ATLM are not required for the ATLM to be OPERABLE.

The purpose of the RWM is to ensure control rod patterns during startup are such that only specified control rod sequences and relative positions are allowed over the operating range from all control rods inserted to just below the low power setpoint (LPSP). The sequences enforced by the RWM effectively limit the potential amount and rate of reactivity increase during a RWE.

The RWM Function of the RC&IS will initiate control rod withdrawal and insert blocks when the actual sequence deviates beyond allowances from the specified sequence. The rod block logic circuitry is the same as that described above. The RC&IS also uses the APRM signals to determine when THERMAL POWER is less than or equal to the LPSP to enable the RWM rod block Function.

The purpose of the MRBM is to limit control rod withdrawal if local power changes during rod withdrawal exceed a preset rod block setpoint. It is assumed to function to block further control rod withdrawal to prevent fuel damage by ensuring that the MCPR and MLHGR do not violate fuel thermal safety limits. The MRBM supplies a trip signal to the RAPI subsystem of RC&IS to appropriately inhibit control rod withdrawal during power operations above the ATLM enable setpoint. There are two MRBM channels, either of which can initiate a control rod block when local neutron flux exceeds the rod block setpoint. The rod block logic circuitry in the RC&IS is arranged as two redundant and separate logic circuits. Control rod withdrawal is permitted only when the two channels agree, unless one of the channels of logic has been manually bypassed. Control rod position, LPRM, and APRM data are the primary data input for the MRBM. APRM signals are used to determine when THERMAL POWER is greater than or equal to the ATLM enable setpoint to enable the MRBM rod block Function.

BASES

BACKGROUND (continued)

With the reactor mode switch in the shutdown position, a control rod withdrawal block is applied to all control rods to ensure that the shutdown condition is maintained. This Function prevents criticality resulting from inadvertent control rod withdrawal during MODE 3, 4, or 5, or during MODE 6 when the reactor mode switch is required to be in the shutdown position. A rod block in either of the two channels of RC&IS will provide a control rod block to all control rods.

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

1.a. Automated Thermal Limit Monitor (ATLM)

The ATLM is designed to prevent violation of the OLMCPR, the SLMCPR, and the cladding 1% plastic strain fuel design limit that may result from a RWE event. The RWE analysis during power operations is discussed in Reference 4. A statistical analysis of RWE events was performed to determine the fuel operating thermal performance response as a function of withdrawal distance and initial operating conditions. From these responses, coefficients used in the ATLM algorithms to calculate rod block setpoints were established. Each ATLM channel has two independent fuel operating thermal limit monitoring functions. One function enforces the OLMCPR, another function enforces the OLMLHGR. The rod block algorithm and setpoints of the ATLM are based on actual on line core fuel operating thermal limit information. If instantaneous LPRM data, which are fed to the ATLM, exceed the calculated rod block setpoints, a rod block signal is issued.

The Automated Thermal Limit Monitor satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

Two channels of the ATLM are available and are required to be OPERABLE to ensure that no single instrument failure can preclude a rod block from this Function. The OPERABILITY of the ATLM depends on the OPERABILITY of the inputs and devices required to produce a rod block. The required inputs and devices are as described in Reference 1.

The ATLM is assumed to mitigate the consequences of a RWE event when THERMAL POWER is greater than or equal to the ATLM enable setpoint (≥ 30% RTP). Below this power level, the consequences of an RWE event will not exceed the Fuel Cladding Integrity Safety Limit (FCISL), and therefore the ATLM is not required to be OPERABLE.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

1.b. Rod Worth Minimizer (RWM)

The RWM enforces the Gang Withdrawal Sequence Restrictions (GWSR) to ensure that the initial conditions of the RWE analysis are not violated. The analytical methods and assumptions used in evaluating the RWE are summarized in Reference 5. The GWSR assure that control rod worths are maintained to within reasonable values by only allowing rod patterns that result in relatively low rod worths when control rods are withdrawn. Requirements that the control rod sequence is in compliance with GWSR are specified in LCO 3.1.6, "Rod Pattern Control."

The RWM Function satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

The RWM is a backup to operator control of control rod sequences, or reference rod pull sequence (RRPS) for automated or semi-automatic operation. However, the RWM is designed as a dual channel system and both channels are required to be OPERABLE for automatic operation. Required Actions of LCO 3.1.3, "Control Rod OPERABILITY" and LCO 3.1.6 may necessitate bypassing individual control rods in the RAPI subsystem to allow continued operation with inoperable control rods or to allow correction of a control rod pattern not in compliance with GWSR. The individual control rods may be bypassed as required by the conditions and the RWM is not considered inoperable provided SR 3.3.2.1.9 is met.

Compliance with the GWSR, and therefore OPERABILITY of the RWM, is required in MODES 1 and 2 when THERMAL POWER is less than or equal to the LPSP (≤ 10% RTP). Above this power level, there is no possible control rod configuration that results in a control rod worth that could exceed the 712 J/g (170 cal/g) fuel-damage limit during a RWE. In MODES 3, 4 and 5, all control rods are required to be inserted in the core. In MODE 6, since only one or two control rods associated with the same hydraulic control unit can be withdrawn from a core cell containing fuel assemblies, adequate SHUTDOWN MARGIN ensures that the consequences of a RWE are acceptable, since the reactor will be subcritical.

1.c Multi-Channel Rod Block (MRBM)

The MRBM is assumed to function to block further control rod withdrawal to prevent fuel damage by ensuring that the MCPR and MLHGR do not violate fuel thermal safety limits during an RWE conservatively assuming

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

neither ATLM channel stops the continued withdrawal of rods. The RWE analysis during power operations is discussed in Reference 4. The MRBM logic receives inputs from the LPRMs, the APRMs, and control rod status data to determine when rod withdrawal blocks are required. The MRBM monitors the core in 4-by-4 fuel bundle regions where control rods are being withdrawn. The MRBM algorithm covers the monitoring of multiple regions simultaneously depending on the size of the gang of control rods being withdrawn. The MRBM uses the LPRM signals to detect local power changes during control rod withdrawal, and issues a block if the MRBM signal exceeds a preset rod block setpoint.

The Multi-Channel Rod Block Monitor satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

Two channels of the MRBM are available and are required to be OPERABLE to ensure that no single instrument failure can preclude a rod block from this Function. The OPERABILITY of the MRBM depends on the OPERABILITY of the inputs and devices required to produce a rod block. The required inputs and devices are as described in Reference 1.

The MRBM is assumed to mitigate the consequences of a RWE event when THERMAL POWER is greater than or equal to the ATLM enable setpoint (≥ 30% RTP). Below this power level, the consequences of an RWE event will not exceed the FCISL, and therefore the MRBM is not required to be OPERABLE.

2. Reactor Mode Switch - Shutdown Position

During MODES 3, 4 and 5, and during MODE 6 when the Reactor Mode Switch is required to be in the shutdown position, the core is assumed to be subcritical; therefore, no positive reactivity insertion events are analyzed. The Reactor Mode Switch - Shutdown Position control rod withdrawal block ensures that the reactor remains subcritical by blocking control rod withdrawal, thereby preserving the assumptions of the safety analysis.

The Reactor Mode Switch - Shutdown Position Function satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

Two channels are required to be OPERABLE to ensure that no single channel failure will preclude a rod block when required. There is no Allowable Value for this Function since the channels are mechanically actuated based solely on reactor mode switch position.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

During shutdown conditions (MODE 3, 4, 5, or 6) no positive reactivity insertion events are analyzed because assumptions are that control rod withdrawal blocks are provided to prevent criticality. Therefore, when the reactor mode switch is in the shutdown position, the control rod withdrawal block is required to be OPERABLE. During MODE 6 with the reactor mode switch in the refuel position and RC&IS single/gang selection switch in “single”, the one rod-out interlock (LCO 3.9.2, "Refuel Position One-Rod/Rod-Pair-Out Interlock") provides the required control rod withdrawal blocks.

ACTIONS

A.1

With one required ATLM channel inoperable, the remaining OPERABLE channel is adequate to perform the control rod block function; however, overall reliability is reduced because a single failure in the remaining OPERABLE channel can result in no control rod block capability for the ATLM. For this reason, Required Action A.1 requires restoration of the inoperable required channel to OPERABLE status. The 7-day Completion Time for restoring ATLM to OPERABLE status is based on the low probability of an event occurring coincident with a failure in the remaining OPERABLE channel.

B.1

With one required RWM channel inoperable, the remaining OPERABLE channel is adequate to perform the control rod block function; however, overall reliability is reduced because a single failure in the remaining OPERABLE channel can result in no control rod block capability for the RWM. For this reason, Required Action B.1 requires restoration of the inoperable required channel to OPERABLE status. The 7 day Completion Time for restoring RWM to OPERABLE status is based on the low probability of an event occurring coincident with a failure in the remaining OPERABLE channel.

C.1

With one required MRBM channel inoperable, the remaining OPERABLE channel is adequate to perform the control rod block function; however, overall reliability is reduced because a single failure in the remaining OPERABLE channel can result in no control rod block capability for the MRBM. For this reason, Required Action C.1 requires restoration of the

BASES

ACTIONS (continued)

inoperable required channel to OPERABLE status. The 7 day Completion Time for restoring MRBM to OPERABLE status is based on the low probability of an event occurring coincident with a failure in the remaining OPERABLE channel.

D.1

If Required Action A.1 or Required Action B.2 is not met and the associated Completion Time has expired, control rod withdrawal must be suspended immediately. In addition, if two required ATLM channels, or two required RWM channels, or two required MRBM channels are inoperable, the ATLM, or the RWM, or the MRBM is not capable of performing its intended function; thus, control rod withdrawal must also be suspended immediately. This ensures erroneous control rod withdrawal does not occur.

E.1 and E.2

With one required Reactor Mode Switch - Shutdown Position control rod withdrawal block channel inoperable, the remaining OPERABLE channel is adequate to perform the control rod withdrawal block function. However, since the Required Actions are consistent with the normal action of an OPERABLE Reactor Mode Switch - Shutdown Position Function (i.e., maintaining all control rods inserted), there is no distinction between having one or two channels inoperable.

In both cases (one or both required channels inoperable), suspending all control rod withdrawal and initiating action to fully insert all insertable control rods in core cells containing one or more fuel assemblies will ensure that the core is subcritical with adequate SDM ensured by LCO 3.1.1, "SHUTDOWN MARGIN (SDM)." Control rods in core cells containing no fuel assemblies do not affect the reactivity of the core and, therefore, are not required to be inserted. Action must continue until all insertable control rods in core cells containing one or more fuel assemblies are fully inserted.

SURVEILLANCE REQUIREMENTS

As noted at the beginning of the Surveillance Requirements, the SRs for each Control Rod Block instrumentation Function are found in the SRs column of Table 3.3.2.1-1.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The Surveillances are modified by a Note to indicate that a required ATLM, RWM, or MRBM channel may be placed in an inoperable status solely for performance of required Surveillances and entry into associated Conditions and Required Actions may be delayed up to 6 hours provided the associated Function maintains control rod block capability. Upon completion of the Surveillance, or expiration of the 6 hour allowance, the required channel must be returned to OPERABLE status or the applicable Condition entered and Required Actions taken. The allowance of this Note is based on the reliability of the channels and the average time required to perform the channel Surveillance, and the low probability of an event occurring coincident with a failure in the remaining OPERABLE channels.

SR 3.3.2.1.1

A CHANNEL FUNCTIONAL TEST is performed for each required ATLM channel to ensure that the entire channel will perform the intended function. It includes the RC&IS inputs. The associated controllers, displays, monitoring and input/output (I/O) communication interfaces continuously function during normal power operation. Abnormal operation of these components is detected and alarmed. In addition, the associated controllers are equipped with on-line diagnostic capabilities for cyclically monitoring the functionality of I/O signals, buses, power supplies, processors, and inter-processor communications.

The Frequency of 31 days is based on the reliability of the channels.

As noted in the SR, SR 3.3.2.1.1 is not required to be performed until 1 hour after THERMAL POWER is ≥ 30% RTP. This allows THERMAL POWER to be increased to ≥ 30% RTP to perform the required Surveillance if the 31-day Frequency is not met per SR 3.0.2. The 1-hour allowance is based on operating experience and in consideration of providing a reasonable time in which to complete the SRs.

SR 3.3.2.1.2 and SR 3.3.2.1.3

A CHANNEL FUNCTIONAL TEST is performed for each required RWM channel to ensure that the entire system will perform the intended function. The CHANNEL FUNCTIONAL TEST for the RWM is performed by attempting to withdraw a control rod not in compliance with the prescribed sequence and verifying a control rod block occurs. The associated controllers, displays, monitoring and input/output (I/O)

BASES

SURVEILLANCE REQUIREMENTS (continued)

communication interfaces continuously function during normal power operation. Abnormal operation of these components is detected and alarmed. In addition, the associated controllers are equipped with on-line diagnostic capabilities for cyclically monitoring the functionality of I/O signals, buses, power supplies, processors, and inter-processor communications.

As noted in the SR, SR 3.3.2.1.2 is not required to be performed until 1 hour after any control rod is withdrawn in MODE 2. As noted in the SR, SR 3.3.2.1.3 is not required to be performed until 1 hour after THERMAL POWER is ≤ 10% RTP. This allows entry into MODE 2 for SR 3.3.2.1.2, and THERMAL POWER to be decreased to ≤ 10% for SR 3.3.2.1.3, to perform the required Surveillance if the 31-day Frequency is not met per SR 3.0.2. The 1-hour allowance is based on operating experience and in consideration of providing a reasonable time in which to complete the SRs. The Frequencies of 31 days are based on the reliability of the channels.

SR 3.3.2.1.4

A CHANNEL FUNCTIONAL TEST is performed for each required MRBM channel to ensure that the entire channel will perform the intended function. It includes the RC&IS inputs. The associated controllers, displays, monitoring and input/output (I/O) communication interfaces continuously function during normal power operation. Abnormal operation of these components is detected and alarmed. In addition, the associated controllers are equipped with on-line diagnostic capabilities for cyclically monitoring the functionality of I/O signals, buses, power supplies, processors, and inter-processor communications.

The Frequency of 31 days is based on the reliability of the channels.

As noted in the SR, SR 3.3.2.1.4 is not required to be performed until 1 hour after THERMAL POWER is ≥ 30% RTP. This allows THERMAL POWER to be increased to ≥ 30% RTP to perform the required Surveillance if the 31-day Frequency is not met per SR 3.0.2. The 1-hour allowance is based on operating experience and in consideration of providing a reasonable time in which to complete the SRs.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.2.1.5

The required RWM channels are bypassed when power is above a specified value (LPSP). The power level is determined from the APRM signals. The RWM bypass setpoint must be verified periodically to be > 10% RTP (i.e., the RWM is not bypassed at or below the LPSP). If the RWM LPSP is nonconservative, then the affected RWM channel is considered inoperable. Alternatively, each required RWM channel associated with a nonconservative RWM LPSP can be placed in the conservative condition (manually enabled). If manually enabled, the SR is met and the affected RWM channel is not considered inoperable.

SR 3.3.2.1.6

The required ATLM channels are bypassed when power is below a specified value (ATLM enable setpoint). The power level is determined from the APRM signals. The ATLM bypass setpoint must be verified periodically to be < 30% RTP (i.e., the ATLM is not bypassed at or above the ATLM enable setpoint). If the ATLM enable setpoint is nonconservative, then the affected ATLM channel is considered inoperable. Alternatively, each required ATLM channel associated with a nonconservative ATLM enable setpoint can be placed in the conservative condition (manually enabled). If manually enabled, the SR is met and the affected ATLM channel is not considered inoperable.

SR 3.3.2.1.7

The required MRBM channels are bypassed when power is below a specified value (ATLM enable setpoint). The power level is determined from the APRM signals. The MRBM bypass setpoint must be verified periodically to be < 30% RTP (i.e., the MRBM is not bypassed at or above the ATLM enable setpoint). If the ATLM enable setpoint is nonconservative, then the affected MRBM channel is considered inoperable. Alternatively, each required MRBM channel associated with a nonconservative ATLM enable setpoint can be placed in the conservative condition (manually enabled). If manually enabled, the SR is met and the affected MRBM channel is not considered inoperable.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.2.1.8

The CHANNEL FUNCTIONAL TEST for the Reactor Mode Switch - Shutdown Position control rod withdrawal block is performed by attempting to withdraw any control rod with the reactor mode switch in the shutdown position and verifying that a control rod block occurs.

As noted in the SR, the Surveillance is only required to be performed until 1 hour after the reactor mode switch is in the shutdown position, since testing of this interlock with the reactor mode switch in any other position cannot be performed without using jumpers, lifted leads or moveable links. This allows entry into MODES 3, 4, 5, and 6 if the 24-month Frequency is not met per SR 3.0.2. The 1-hour allowance is based on operating experience and in consideration of providing a reasonable time in which to complete the SRs.

The 24-month Surveillance 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 24-month Frequency.

SR 3.3.2.1.9

LCO 3.1.3 and LCO 3.1.6 may require individual control rods to be bypassed in the RC&IS cabinets to allow insertion of an inoperable control rod or correction of a control rod pattern not in compliance with GWSR. With the control rods bypassed in the RC&IS cabinets, the RWM will not control the movement of these bypassed control rods. To ensure the proper bypassing and movement of those affected control rods, a second licensed operator or other qualified member of the technical staff must verify the bypassing and movement of these control rods. Compliance with this SR allows the RWM to be OPERABLE with these control rods bypassed.

BASES

REFERENCES	1.	Subsection 7.7.2.
	2.	Subsection 15.2.1
	3.	Subsection 15.3.1.
	4.	Subsection 15.3.9.
	5.	Subsection 15.3.8.

B 3.3 INSTRUMENTATION

B 3.3.3.1 Remote Shutdown System

BASES

BACKGROUND

The Remote Shutdown System provides instrumentation and controls outside the main control room to allow prompt hot shutdown of the reactor and to maintain safe conditions during hot shutdown, which can be accomplished from either one of two remote shutdown panels. This capability is necessary to protect against the possibility of the control room becoming inaccessible. It also provides capability for subsequent cold shutdown of the reactor through the use of suitable procedures.

The operational functions needed for remote shutdown control of a system are provided on the remote shutdown panels. All parameters that can be displayed/controlled from Division 1 and Division 2 in the Main Control Room, and that are necessary to follow the status of the reactor plant, are also displayed/controlled from the corresponding divisional displays at each remote shutdown panel. The individual system equipment and instrumentation that interface with the Remote Shutdown System are listed in Reference 2. The two remote shutdown panels are located in two different areas and different rooms inside the Reactor Building.

The Remote Shutdown System provides sufficient redundancy in the control and monitoring capability to accommodate a single failure in the interfacing systems and the Remote Shutdown System controls, in addition to the single-failure event that caused the control room evacuation. The Remote Shutdown System is designed to prevent degrading the capability of the interfacing systems.

Normally, the turbine bypass valves automatically control reactor pressure, and the reactor feedwater system automatically maintains vessel water level. With these functions available, reactor cooldown is achieved through the normal heat sinks. This cooldown process can be supplemented from the remote shutdown panel using the Reactor Water Cleanup/Shutdown Cooling (RWCU/SDC) System. The RWCU/SDC System provides the capability to bring the reactor from a high-pressure condition to cold shutdown. Control of both RWCU/SDC trains is provided on either remote shutdown panel. The Reactor Closed Cooling Water (RCCW) System is aligned to provide cooling water to the RWCU/SDC non-regenerative heat exchangers, and the Plant Service Water (PSW) System is aligned to cool the RCCW heat exchangers. Control of two RCCW trains and two PSW trains is provided on either remote shutdown panel.

BASES

BACKGROUND (continued)

If the reactor feedwater system is not available, control of the Control Rod Drive (CRD) System is provided on the remote shutdown panels. Control of the high-pressure makeup injection capability of the CRD System ensures that the vessel water level remains above the Automatic Depressurization System trip setpoint and above the elevation of the RWCU/SDC mid-vessel suction line nozzle. If main steam line isolation occurs, the Isolation Condenser System (ICS) automatically controls reactor pressure. Because the logic processing equipment for the ICS (or any other safety or nonsafety-related system) is outside the Main Control Room, ICS operation is not affected by an event necessitating control room evacuation, and continued operation of the isolation condensers is assured. If the event necessitating control room evacuation results in a loss of the pressure regulator, but does not cause main steam line isolation, the ICS would initiate on high pressure. With the ICS in operation, the isolation condensers provide initial decay heat removal, and further reactor cooldown is achieved from the remote shutdown panels using the RWCU/SDC.

In the event that the control room becomes inaccessible, the operators can establish control at either remote shutdown panel and place and maintain the plant in MODE 3. The plant automatically reaches MODE 3 following a plant shutdown and can be maintained safely in MODE 3 for an extended period of time.

The OPERABILITY of the Remote Shutdown System control and instrumentation Functions ensures that there is sufficient information available on selected plant parameters to place and maintain the plant in MODE 3, from either one of two remote shutdown panels, should the control room become inaccessible.

APPLICABLE SAFETY ANALYSES

The Remote Shutdown System is required to provide equipment at appropriate locations outside the control room with a design capability to promptly shut down the reactor to MODE 3, including the necessary instrumentation and controls to maintain the plant in a safe condition in MODE 3.

The criteria governing the design and the specific system requirements of the Remote Shutdown System are located in 10 CFR 50, Appendix A, GDC 19 (Ref. 1).

BASES

APPLICABLE SAFETY ANALYSES (continued)

The only action required to promptly shutdown the reactor to MODE 3 and maintain the plant in a safe condition in MODE 3 is a manual scram of the plant. If the operator is not able to initiate manual scram from the main control room prior to a required evacuation, manual scram can be initiated from either of the remote shutdown panels. Therefore, the Division 1 & 2 Manual Scram Switches at any one of the remote shutdown panels are required to be OPERABLE.

The Remote Shutdown System satisfies Criterion 4 of 10 CFR 50.36(c)(2)(ii).

LCO

The Remote Shutdown System LCO provides the requirements for the OPERABILITY of the instrumentation and controls Functions necessary to place and maintain the plant in MODE 3 from a location other than the control room. The controls and instrumentation Functions are the Reactor Protection System (RPS) Division 1 and Division 2 Manual Scram Switches.

The Remote Shutdown System is OPERABLE if all instrument and control channels associated with the DC and Uninterruptible AC Electrical Power Distribution Divisions required by LCO 3.8.6, "Distribution Systems – Operating," needed to support the remote shutdown function are OPERABLE for one of the two remote shutdown panels.

This LCO is intended to ensure that the instruments and control circuits will be OPERABLE if plant conditions require that the Remote Shutdown System be placed in operation.

APPLICABILITY

The Remote Shutdown System LCO is applicable in MODES 1 and 2. This is required so that the plant can be placed and maintained in MODE 3 for an extended period of time from a location other than the control room.

This LCO is not applicable in MODES 3, 4, 5, and 6. In these MODES, the plant is already subcritical and in a condition of reduced Reactor Coolant System energy. Under these conditions, considerable time is available to restore necessary instrument control Functions if control room instruments or control becomes unavailable. Consequently, TS do not require OPERABILITY in MODES 3, 4, 5, and 6.

BASES

ACTIONS	A Note has been provided to modify the ACTIONS related to Remote Shutdown System Functions. Section 1.3, Completion Times, specifies that once a Condition has been entered, subsequent divisions, subsystems, components, or variables expressed in the Condition, discovered to be inoperable or not within limits, will not result in separate entry into the Condition. Section 1.3 also specifies that Required Actions of the Condition continue to apply for each additional failure, with Completion Times based on initial entry into the Condition. However, the Required Actions for inoperable Remote Shutdown System Functions provide appropriate compensatory measures for separate Functions. As such, a Note has been provided that allows separate Condition entry for each inoperable Remote Shutdown System Function. <u>A.1</u> Condition A addresses the situation where one or more required Functions is inoperable. This includes the controls for any required Function. The Required Action is to restore the required Function to OPERABLE status within 30 days. The Completion Time is based on operating experience and the low probability of an event that would require evacuation of the control room. <u>B.1</u> If the Required Action and associated Completion Time of Condition A are not met, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 12 hours. The allowed Completion Time is 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	<u>SR 3.3.3.1.1</u> A CHANNEL FUNCTIONAL TEST is performed on the Division 1 and Division 2 Manual Scram Switches to ensure that each switch will perform the intended Function. The Frequency of 24 months is based on the reliability of the RPS actuation logic and controls.

BASES

REFERENCES	1.	10 CFR 50, Appendix A, GDC 19.
	2.	Subsection 7.4.2.

B 3.3 INSTRUMENTATION

B 3.3.3.2 Post-Accident Monitoring (PAM) Instrumentation

BASES

BACKGROUND

The purpose of the Post-Accident Monitoring Instrumentation is to display plant variables that provide information required by the control room operators during accident situations. The instruments that monitor these variables are designated as Type A, B, and C in accordance with Regulatory Guide 1.97 (Ref.1).

The OPERABILITY of the accident monitoring instrumentation ensures that there is sufficient information available on selected plant parameters to monitor and assess plant status and behavior following an accident. This capability is consistent with the recommendations of Reference 1.

APPLICABLE SAFETY ANALYSES

The PAM Instrumentation LCO ensures the OPERABILITY of Regulatory Guide 1.97, Type A, variables. Type A variables provide the primary information required to permit the control room operating staff to:

- Take specific planned manually-controlled actions for which no automatic control is provided and that are required for safety systems to perform their safety-related functions as assumed in the plant Accident Analysis Licensing Basis.
- Take specific planned manually-controlled actions for which no automatic control is provided and that are required to mitigate the consequences of an anticipated operational occurrence.

The PAM Instrumentation LCO ensures the OPERABILITY of Regulatory Guide 1.97, Type B, variables. Type B variables are those variables that provide primary information to the control room operators to assess the plant critical safety functions.

The PAM Instrumentation LCO ensures the OPERABILITY of Regulatory Guide 1.97, Type C, variables. Type C variables are those variables that provide primary information to the control room operators to indicate the potential for breach or the actual breach of the three fission product barriers (fuel cladding, reactor coolant pressure system boundary, and containment pressure boundary).

BASES

APPLICABLE SAFETY ANALYSES (continued)

The list of Type A, B, and C PAM variables is developed and maintained in accordance with Specification 5.5.14, "Post-Accident Monitoring (PAM) Instrumentation Program."

PAM instrumentation that meets the definition of Type A in Regulatory Guide 1.97 satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii). PAM instrumentation that meets the definition of Type B or C in Regulatory Guide 1.97 is retained in the Technical Specifications because it is intended to assist operators in minimizing the consequences of accidents. Therefore, these Type B and C variables are important for reducing public risk.

LCO

LCO 3.3.3.2 requires two OPERABLE channels for each Type A, B, and C PAM Instrumentation Function, identified in accordance with Specification 5.5.14 and associated with the DC and Uninterruptible AC Electrical Power Distribution Divisions required by LCO 3.8.6, "Distribution Systems – Operating," to ensure no single failure prevents the operators from being presented with the information necessary to determine the status of the unit and to bring the unit to, and maintain it in, a safe condition following that accident. A minimum of two channels allows a CHANNEL CHECK during the post accident phase to confirm the validity of displayed information.

APPLICABILITY

The PAM Instrumentation LCO is applicable in MODES 1 and 2. These variables are related to the diagnosis and preplanned actions required to mitigate Design Basis Accidents (DBAs). The applicable DBAs are assumed to occur in MODES 1 and 2. In MODES 3, 4, 5, and 6, plant conditions are such that the likelihood of an event that would require PAM instrumentation is extremely low; therefore, PAM instrumentation is not required to be OPERABLE in these MODES.

ACTIONS

A Note has been added to the ACTIONS Table. This Note modifies the ACTIONS related to PAM instrumentation channels. Section 1.3, Completion Times, specifies that once a Condition has been entered, subsequent divisions, subsystems, components, or variables expressed in the Condition discovered to be inoperable or not within limits, will not result in separate entry into the Condition. Section 1.3 also specifies that Required Actions of the Condition continue to apply for

BASES

ACTIONS (continued)

each additional failure, with Completion Times based on initial entry into the Condition. However, the Required Actions for inoperable PAM instrumentation channels provide appropriate compensatory measures for separate Functions. As such, the Note allows separate Condition entry for each inoperable PAM Function.

A.1

When one or more required PAM Functions have one required channel that is inoperable, the required inoperable channel must be restored to OPERABLE status within 30 days. The 30-day Completion Time is based on operating experience and takes into account the remaining OPERABLE channel, the passive nature of the instrument (no critical automatic action is assumed to occur from these instruments), and the low probability of an event requiring PAM instrumentation during this interval.

B.1

If a channel has not been restored to OPERABLE status in 30 days, this Required Action specifies initiation of actions in accordance with Specification 5.6.5, “Post-Accident Monitoring Report,” which requires a written report to be submitted to the NRC. This report discusses the cause of the inoperability and identifies proposed restorative actions. This Action is appropriate in lieu of a shutdown requirement since alternative Actions are identified before loss of functional capability, and given the likelihood of plant conditions that would require information provided by this instrumentation.

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

Condition C applies when one or more required PAM Functions have two required channels inoperable, (i.e., two required channels inoperable in the same Function). Required Action C.1 directs restoration of one required channel to OPERABLE status. Alternatively, Required Actions C.2.1 and C.2.2 require verification that a preplanned alternate method of monitoring the affected PAM Function is available and initiation of actions in accordance with Specification 5.6.5. Required Actions C.2.1 and C.2.2 are appropriate in instances where alternate means of monitoring have been developed and tested. These alternate means may be permanently or temporarily installed and utilized if the normal PAM channel cannot be restored to OPERABLE status within the allotted time. The report provided to the NRC should discuss the alternate means used, describe

BASES

ACTIONS (continued)

the degree to which the alternate means are equivalent to the installed PAM channels, justify the areas in which they are not equivalent, and provide a schedule for restoring the normal PAM channels.

The Completion Time of 7 days is based on the relatively low probability of an event requiring PAM instrument operation.

D.1

If the Required Actions and associated Completion Times of Condition C cannot be met, the plant must be placed in a MODE where the LCO does not apply. This is done by placing the plant in at least MODE 3 within 12 hours. The allowed Completion Time is reasonable, based on operating experience, to reach the required plant condition from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.3.3.2.1

Performance of the CHANNEL CHECK once every 31 days ensures that a gross instrumentation failure 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 required 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 isolation, indication, and readability. If a required channel is outside the match criteria, it may be an indication that the sensor or the signal-processing equipment has drifted outside its limit. Performance of the CHANNEL CHECK guarantees that undetected channel failure is limited to 31 days.

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 required channel of a given function in any 31 day interval is rare. The CHANNEL CHECK supplements less

BASES

SURVEILLANCE REQUIREMENTS (continued)

formal, but more frequent, checks of channels during normal operational use of those displays associated with the required channels of this LCO.

SR 3.3.3.2.2

A CHANNEL CALIBRATION is performed at every 24 months for each required channel. CHANNEL CALIBRATION is a complete check of the instrument loop including the sensor. The test verifies that the channel responds to measured parameter with the necessary range and accuracy. The Frequency is based on operating experience and consistency with the typical industry refueling cycles.

REFERENCES

1. Regulatory Guide 1.97, “Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants,” Revision 4, June 2006.

B 3.3 INSTRUMENTATION

B 3.3.4.1 Reactor Coolant System (RCS) Leakage Detection Instrumentation

BASES

BACKGROUND

GDC 30 of 10 CFR 50, Appendix A (Ref. 1), requires means for detecting and, to the extent practical, identifying the location of the source of RCS LEAKAGE. Regulatory Guide 1.45 (Ref. 2) describes acceptable methods for selecting leakage detection systems.

Limits on LEAKAGE from the reactor coolant pressure boundary (RCPB) are required so that appropriate action can be taken before the integrity of the RCPB is impaired (Ref. 2). Leakage detection systems for the RCS are provided to alert the operators when leakage rates above normal background levels are detected and also to supply quantitative measurement of rates. The Bases for LCO 3.4.2, "RCS Operational LEAKAGE," discuss the limits on RCS LEAKAGE rates.

Systems for separating the LEAKAGE of an identified source from an unidentified source are necessary to provide prompt and quantitative information to the operators to permit them to take immediate corrective action.

LEAKAGE from the RCPB inside the drywell is detected by the drywell floor drain high conductivity waste (HCW) sump monitoring system, the drywell air cooler condensate flow monitoring, and the particulate channel of the drywell fission product monitoring system. The primary means of quantifying LEAKAGE in the drywell is the HCW sump monitoring system.

The drywell floor drain HCW sump collects unidentified leakage from such sources as floor drains, valve flanges, closed component cooling water for reactor equipment, condensate from the drywell air coolers and from any leakage not connected to the drywell equipment drain sump. The sump is equipped with two pumps and special monitoring instrumentation that measures the pump’s operating frequency, the sump level and flow rates. These measurements are provided on a continuous basis to the main control room. The sump instrumentation is designed with the sensitivity to detect a leakage step-change (increase) of 3.8 liters/min (1.0 gpm) within one hour and alarm at flow rates in excess of 19 liters/min (5 gpm).

The condensate flow rate from the drywell air coolers is monitored for high drain flow, which could be indicative of leaks from piping or the equipment within the drywell. This flow is monitored by one instrumented channel using a bucket type flow transmitter located in the drywell. The

BASES

BACKGROUND (continued)

flow measurement is provided to the main control room on a continuous basis for recording and alarming.

Primary coolant leaks and radioactivity within the drywell are detected through sampling and monitoring of the drywell atmosphere by the Process Radiation Monitoring System (PRMS). The fission product monitor samples for radioactive particulates. The radiation levels are recorded in the main control room and alarmed on abnormally high concentration levels.

APPLICABLE SAFETY ANALYSES

A threat of significant compromise to the RCPB exists if the barrier contains a crack that is large enough to propagate rapidly. LEAKAGE rate limits are set low enough to detect the LEAKAGE emitted from a single crack in the RCPB (Ref. 3). Each of the leakage detection systems inside the drywell is designed with the capability of detecting LEAKAGE less than the established LEAKAGE rate limits and providing appropriate alarm of excess LEAKAGE in the control room.

A control room alarm allows the operators to evaluate the significance of the indicated LEAKAGE and, if necessary, shut down the reactor for further investigation and corrective action. The allowed LEAKAGE rates are well below the rates predicted for critical crack sizes (Ref. 3). Therefore, these actions provide adequate response before a significant break in the RCPB can occur.

RCS leakage detection instrumentation satisfies Criterion 1 of 10 CFR 50.36(c)(2)(ii).

LCO

The drywell floor drain HCW sump monitoring system is required to quantify the unidentified LEAKAGE from the RCS. Thus, for the system to be considered OPERABLE, either the flow monitoring or the sump level monitoring portion of the system must be OPERABLE. The other monitoring systems provide early alarms to the operators so closer examination of other detection systems will be made to determine the extent of any corrective action that may be required. With the leakage detection systems inoperable, monitoring for LEAKAGE in the RCPB is degraded.

BASES

APPLICABILITY

In MODES 1, 2, 3, and 4, leakage detection systems are required to be OPERABLE to support LCO 3.4.2. This Applicability is consistent with that for LCO 3.4.2.

ACTIONS

A.1

With the drywell floor drain HCW sump monitoring system inoperable, no other form of sampling can provide the equivalent information to quantify leakage. However, the drywell air cooler condensate flow monitoring and the drywell fission product monitoring system will provide indications of changes in leakage. With the drywell floor drain HCW sump monitoring system inoperable, but with RCS unidentified and total LEAKAGE being determined every 12 hours (SR 3.4.2.1), operation may continue for 30 days. The 30 day Completion Time of Required Action A.1 is acceptable, based on operating experience, considering the multiple forms of leakage detection that are still available.

B.1

With the drywell fission product monitoring system particulate channel inoperable, grab samples of the drywell atmosphere shall be taken and analyzed to provide periodic leakage information. Provided a sample is obtained and analyzed every 12 hours, the plant may continue operation since at least one other form of drywell leakage detection (i.e., air cooler condensate flow rate monitor) is available. The 12-hour interval provides periodic information that is adequate to detect LEAKAGE.

C.1

With the drywell air cooler condensate flow rate monitoring system inoperable, SR 3.3.4.1.1 is performed every 8 hours to provide periodic information of activity in the drywell at a more frequent interval than the routine Frequency of SR 3.3.4.1-1. The 8-hour interval provides periodic information that is adequate to detect LEAKAGE and recognizes that other forms of leakage detection are available. However, this Required Action is modified by a Note that allows this action to be not applicable if the drywell fission product monitoring system particulate channel is inoperable. Consistent with SR 3.0.1, Surveillances are not required to be performed on inoperable equipment.

BASES

ACTIONS (continued)

D.1 and D.2

With both the drywell fission product monitoring system particulate channel and the drywell air cooler condensate flow rate monitor inoperable, the only means of detecting LEAKAGE is the drywell floor drain HCW sump monitoring system. This Condition does not provide the required diverse means of leakage detection. The Required Action is to restore either of the inoperable monitors to OPERABLE status within 30 days to regain the intended leakage detection diversity. The 30-day Completion Time ensures that the plant will not be operated in a degraded configuration for a lengthy time period.

E.1 and E.2

If any Required Action and associated Completion Time of Condition A, B, C, or D cannot be met or if all required monitors are inoperable 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 12 hours and to MODE 5 within 36 hours. The Completion Time is reasonable, based on plant design, to reach required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.3.4.1.1

Performance of the CHANNEL CHECK once every 12 hours ensures that a gross failure of instrumentation has not occurred. The associated controllers, displays, monitoring and input/output (I/O) communication interfaces continuously function during normal power operation. Abnormal operation of these components is detected and alarmed. In addition, the associated controllers are equipped with on-line diagnostic capabilities for cyclically monitoring the functionality of I/O signals, buses, power supplies, processors, and inter-processor communications.

A CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

The Frequency is based upon operating experience that demonstrates channel failure is rare.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The CHANNEL CHECKs every 12 hours supplement less formal, but more frequent, checks of channels during normal operational use of the displays associated with the channels required by the LCO.

SR 3.3.4.1.2

This SR requires the performance of a CHANNEL FUNCTIONAL TEST of the required RCS leakage detection instrumentation. The test ensures that the required channels can perform their intended function.

The associated controllers, displays, monitoring and input/output (I/O) communication interfaces continuously function during normal power operation. Abnormal operation of these components is detected and alarmed. In addition, the associated controllers are equipped with on-line diagnostic capabilities for cyclically monitoring the functionality of I/O signals, buses, power supplies, processors, and inter-processor communications.

The Frequency of 31 days is based on instrument reliability.

SR 3.3.4.1.3

This SR requires the performance of a CHANNEL CALIBRATION of the required RCS leakage detection instrumentation channels. The calibration verifies the accuracy of the instrument string, including the instruments located inside the drywell. The Frequency of 24 months is a typical refueling cycle and considers channel reliability. Operating experience has proven this Frequency is acceptable.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 30.
2. Regulatory Guide 1.45, May 1973.
3. Section 5.2.5.

B 3.3 INSTRUMENTATION

B 3.3.5.1 Emergency Core Cooling System (ECCS) Instrumentation

BASES

BACKGROUND

The purpose of the ECCS instrumentation is to initiate appropriate responses from the ECCS to ensure that fuel is adequately cooled in the event of an anticipated operational occurrence or accident.

The ECCS instrumentation actuates the Automatic Depressurization System (ADS), the Gravity-Driven Cooling System (GDCS), and Standby Liquid Control (SLC). The equipment involved with ADS is described in the Bases for LCO 3.5.1, “ADS - Operating.” The equipment involved with GDCS is described in the Bases for LCO 3.5.2, “GDCS - Operating.” The equipment involved with SLC is described in the Bases for LCO 3.1.7, “Standby Liquid Control (SLC) System.”

Technical Specifications are required by 10 CFR 50.36 to contain limiting safety system settings (LSSS) defined by the regulation as "...settings for automatic protective devices related to those variables having significant safety functions." Where LSSS is specified for a variable on which a Safety Limit (SL) has been placed, the setting must be chosen such that automatic protective action will correct the abnormal situation before a SL is exceeded. The Analytical Limit is the limit of the process variable at which a safety action is initiated, as established by the safety analysis, to ensure that a SL is not exceeded. Any automatic protection action that occurs on reaching the Analytical Limit therefore ensures that the SL is not exceeded. Where LSSS is specified for a variable having a significant safety function but which does not protect SLs, the setting must be chosen such that automatic protective actions will initiate consistent with the design basis. The Design Limit is the limit of the process variable at which a safety action is initiated to ensure that these automatic protective devices will perform their specified safety function.

The actual settings for automatic protective devices must be chosen to be more conservative than the Analytical / Design Limit to account for instrument loop uncertainties related to the setting at which the automatic protective action would actually occur. The methodology for determining the actual settings, and the required tolerances to maintain these settings conservative to the Analytical / Design Limits, including the requirements for determining that the channel is OPERABLE, are defined in the Setpoint Control Program (SCP), in accordance with Specification 5.5.11, “Setpoint Control Program (SCP)."

BASES

BACKGROUND (continued)

The Limiting Trip Setpoint (LTSP) is a predetermined setting for a protective device chosen to ensure automatic actuation prior to the process variable reaching the Analytical / Design Limit and thus ensuring that the SL would not be exceeded (i.e., for Analytical Limits), or that automatic protective actions occur consistent with the design basis (i.e., for Design Limits). As such, the LTSP accounts for process and primary element measurement errors, and uncertainties in setting the device (e.g., calibration), uncertainties in how the device might actually perform (e.g., accuracy), changes in the point of action of the device over time (e.g., drift during surveillance intervals), and any other factors that may influence its actual performance (e.g., harsh accident environments). In this manner, the LTSP ensures that SLs are not exceeded and that automatic protective devices will perform their specified safety function. As such, the LTSP meets the definition of an LSSS. The nominal trip setpoint to which the setpoint is reset after calibration is the $NTSP_F$, which is more conservative than the LTSP and has margin to assure that the Allowable Value is not exceeded during calibration.

Technical Specifications contain values related to the OPERABILITY of equipment required for safe operation of the facility. OPERABLE is defined in Technical Specifications as "...being capable of performing its safety function(s)." For automatic protective devices, the required safety function is to ensure that a SL is not exceeded and that automatic protective actions will initiate consistent with the design basis. Therefore, the LTSP is the LSSS as defined by 10 CFR 50.36. However, use of the LTSP to define OPERABILITY in Technical Specifications would be an overly restrictive requirement if it were applied as an OPERABILITY limit for the "as-found" value of a protective device setting during a Surveillance.

However, there is also some point beyond which the device would have not been able to perform its function due, for example, to greater than expected drift. This value is specified in the SCP, as required by Specification 5.5.11, in order to define OPERABILITY of the devices and is designated as the Allowable Value which is the least conservative value of the as-found setpoint that a channel can have during CHANNEL CALIBRATION. The LTSP, $NTSP_F$, Allowable Value, "as-found" tolerance, and "as-left" tolerance, and the methodology for calculating the "as-left" and "as-found" tolerances will be maintained in the SCP, as required by Specification 5.5.11.

BASES

BACKGROUND (continued)

The Allowable Value is the least conservative value that the setpoint of the channel can have when tested such that a channel is OPERABLE if the setpoint is found conservative with respect to the Allowable Value during the CHANNEL CALIBRATION. Note that, although a channel is OPERABLE under these circumstances, the setpoint must be left adjusted to a value within the established "as-left" tolerance of the $NTSP_F$ and confirmed to be operating within the statistical allowances of the uncertainty terms assigned in the setpoint calculation. As such, the Allowable Value differs from the $NTSP_F$ by an amount equal to or greater than the "as-found" tolerance value. In this manner, the actual setting of the device will ensure that a SL is not exceeded or that automatic protective actions will initiate consistent with the design basis at any given point of time as long as the device has not drifted beyond that expected during the surveillance interval. If the actual setting of the device is found to be non-conservative with respect to the Allowable Value the device would be considered inoperable from a Technical Specification perspective. This requires corrective action including those actions required by 10 CFR 50.36 when automatic protective devices do not function as required.

As described in Reference 1, the Safety System Logic and Control Engineered Safety Feature (SSLC/ESF) System controls the initiation signals and logic for ECCS. SSLC/ESF is a four-division, separated protection logic system designed to provide a very high degree of assurance to both ensure ECCS initiation when required and prevent inadvertent initiation. Each division of SSLC/ESF is configured such that all functions (e.g., the digital trip module (DTM) function and voter logic unit (VLU) function) are implemented in triply redundant processors to support the requirement that single divisional failures cannot result in inadvertent actuation.

ADS, GDCS (injection and equalizing subsystems), and SLC system actuate in response to a Reactor Vessel Level - Low, Level 1.0 signal sustained for 10 seconds. Additionally, ADS and GDCS injection subsystem actuate in response to a Drywell Pressure - High signal sustained for 60 minutes.

BASES

BACKGROUND (continued)

On receipt of the trip signal the associated actuation logic will seal in and trigger the following sequence of events:

1. For only the Reactor Vessel Level - Low, Level 1.0 sustained signal, both SLC trains actuate after a time delay of 50 seconds on the first Depressurization Valve (DPV) (third ADS timer) injection signal. (The Drywell Pressure - High sustained signal does not initiate SLC trains.)

2. Five of the ten Safety Relief Valves (SRVs) open immediately to start reducing reactor pressure on the first ADS timer injection signal. The remaining five SRVs open after a 10-second time delay on the second ADS timer injection signal.

3. The eight DPVs, which are divided into four groups (group 1 consists of three DPVs, groups 2 and 3 consists of two DPVs each, and group 4 consists of one DPV) open in the following sequence: The first group opens after a 50 second time delay on the first DPV (third ADS timer) injection signal. An additional DPV group opens every 50 seconds on the second through fourth DPV (fourth through sixth ADS timer) injection signals until all of the DPVs are open.

4. All eight squib-actuated valves in the GDCS injection secondary lines open after a 150 second time delay.

5. For only the Reactor Vessel Level - Low, Level 1.0 sustained signal, all four squib-actuated valves in the GDCS equalizing lines, which connect the suppression pool to the reactor pressure vessel (RPV), actuate after a 30-minute time delay if the RPV water level is below Level 0.5. (The Drywell Pressure - High sustained signal does not initiate GDCS equalize subsystem.)

The input trip determinations for all ECCS functions are based upon two-out-of-four logic. The output trip determinations for all ECCS functions are based on the triply redundant logic in the main SSLC/ESF processors transmitting separate close signals to each of the two (for solenoid initiator) or three (for squib initiator) load driver/discrete outputs. The effect is that two of the three triply redundant processors must separately command all of the load drivers/discrete outputs to fire the divisional initiator, making the design single failure proof against inadvertent actuation.

BASES

BACKGROUND (continued)

Four separate multiplexed instrument channels are used to monitor RPV water level for ECCS. Four separate wide range RPV water level sensors and four separate fuel zone water level sensors are utilized to provide input signals for ECCS logic. Signals from the wide range, fuel zone, and drywell pressure sensors are multiplexed at the divisional level and triply redundant sensor data is then transmitted to the SSLC/ESF triply redundant DTM function for setpoint comparison. The DTM functions make a trip/no-trip decision by comparing a digitized analog value against a setpoint and initiating a trip condition for that variable if the setpoint is exceeded. The output of each divisional DTM function (a trip/no-trip condition) is routed to all four divisional triply redundant VLU functions such that each divisional VLU function receives input from each of the four divisional DTM functions.

For maintenance purposes and added reliability, each DTM function has a division of sensors bypass such that all instruments in that division will be bypassed in the trip logic at the VLU functions. Thus, each VLU function will be making its trip decision on a two-out-of-three logic basis for each variable. It is possible for only one division of sensors bypass condition to be in effect at any time.

The processed trip signal from its own division and trip signals from the other three divisions are processed in the triply redundant divisional VLU function for two-out-of-four voting.

The load driver arrangement for actuation of an SRV, DPV squib valve, GDCS secondary branch line squib valve, and suppression pool equalizing line squib valve are given in Reference 1.

Equipment within a single division is powered from the safety-related power source of the same division.

This Specification provides the OPERABILITY requirements for the ECCS instrumentation from the input variable sensors through the DTM function. OPERABILITY requirements for the ECCS actuation circuitry consisting of timers, VLU functions, and load drivers are provided by LCO 3.3.5.2, "Emergency Core Cooling System (ECCS) Actuation." OPERABILITY requirements for actuated components (i.e., squibs and solenoid valves) are addressed in LCO 3.1.7, LCO 3.5.1, and LCO 3.5.2, as appropriate.

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

The actions of the ECCS are explicitly assumed in the safety analyses of Reference 2 and 3. The ECCS is initiated to preserve the integrity of the fuel cladding by limiting the post-LOCA peak cladding temperature to less than the 10 CFR 50.46 limits.

ECCS Instrumentation satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

The OPERABILITY of the ECCS instrumentation is dependent on the OPERABILITY of the individual instrumentation channel Functions specified in Table 3.3.5.1-1. An ECCS instrumentation channel constitutes all of the components within a division of channel sensors. Each Function must have the required number of OPERABLE channels, with setpoints in accordance with the SCP, where appropriate. The actual setpoint is calibrated consistent with the SCP. Each ECCS subsystem must also respond within its assumed response time. A channel is inoperable if its actual trip setpoint is non-conservative with respect to its required Allowable Value.

$NTSP_F$s are specified in the SCP, as required by Specification 5.5.11. The $NTSP_F$s are selected to ensure the actual setpoints are conservative with respect to the Allowable Value between successive CHANNEL CALIBRATIONS. Operation with a trip setpoint less conservative than the $NTSP_F$, but more conservative with respect to its Allowable Value, is acceptable. A channel is inoperable if its actual trip setpoint is non-conservative with respect to its required Allowable Value.

In general, the individual Functions are required to be OPERABLE in the MODES or other specified conditions that may require ECCS initiation to mitigate the consequences of a design basis accident or transient.

Although there are four channels of ECCS instrumentation for each function, only three ECCS instrumentation channels for each function are required to be OPERABLE. The three required channels are those channels associated with the DC and Uninterruptible AC Electrical Power Distribution Divisions required by LCO 3.8.6, "Distribution Systems - Operating," and LCO 3.8.7, "Distribution Systems - Shutdown." This is acceptable because the single-failure criterion is met with three OPERABLE ECCS instrumentation channels, and because each ECCS instrumentation division is associated with and receives power from only one of the four electrical divisions.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

The specific Applicable Safety Analyses, LCO and Applicability discussions for the functions in Table 3.3.5.1-1 are listed below:

1. Reactor Vessel Water Level - Low, Level 1

Reactor Vessel Water Level - Low, Level 1 is the primary signal for the initiation of the ECCS for a steam line break outside containment because fuel damage could result if RPV water level is too low. The Reactor Vessel Water Level - Low, Level 1 is assumed to be OPERABLE and capable of initiating the ADS, GDCS (injection and equalizing subsystems), and SLC during the accidents analyzed in References 2 and 3. The core cooling function of the ECCS, along with the scram action of the RPS, assures that the fuel peak cladding temperature remains below the limits of 10 CFR 50.46.

Three channels of Reactor Vessel Water Level - Low, Level 1 Function are required to be OPERABLE to ensure that no single instrument failure can preclude ECCS initiation. The Level 1 signal is initiated from four wide range level sensors.

2. Reactor Vessel Water Level - Low, Level 0.5

Reactor Vessel Water Level - Low, Level 0.5 signal is used in the ECCS logic as a permissive for actuation of the GDCS suppression equalizing lines valves, after a 30-minute time delay from the Reactor Vessel Level - Low, Level 1.0 sustained signal. The Reactor Vessel Water Level - Low, Level 0.5 is assumed to be OPERABLE and capable of initiating the GDCS suppression pool equalizing line valves following boil-off of RPV inventory during the accidents analyzed in References 2 and 3. The core cooling function of the ECCS, along with the scram action of the RPS, assures that the fuel peak cladding temperature remains below the limits of 10 CFR 50.46.

Three channels of Reactor Vessel Water Level - Low, Level 0.5 Function are required to be OPERABLE to ensure that no single instrument failure can preclude GDCS initiation. Reactor Vessel Water Level - Low, Level 0.5 signals are initiated from four fuel zone level sensors.

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

3. Drywell Pressure - High

Drywell Pressure - High is used for initiation of ADS and GDCS injection subsystem, as some steam line breaks (or breaks above operating water level), and other small breaks will not result in a level reduction to Reactor Vessel Level - Low, Level 1. This is due to the nature of steam line breaks (no rapid loss of vessel water inventory) and the large capability of the reactor feedwater system. The time delay provides sufficient margin to ensure successful event mitigation by automatic actuation.

Three channels of Drywell Pressure - High Function are required to be OPERABLE to ensure that no single instrument failure can preclude ADS and GDCS injection subsystem initiation. Drywell Pressure - High signals are initiated from four drywell pressure sensors.

The Drywell Pressure - High Function is required to be OPERABLE in MODES 1, 2, 3, and 4 consistent with the Applicability for LCO 3.6.1.1, "Containment."

ACTIONS

A Note has been provided to modify the ACTIONS related to ECCS instrumentation channels. Section 1.3, Completion Times, specifies once a Condition has been entered, subsequent divisions, subsystems, components or variables expressed in the Condition discovered to be inoperable or not within limits, will not result in separate entry into the Condition. Section 1.3 also specifies Required Actions of the Condition continue to apply for each additional failure, with Completion Times based on initial entry into the Condition. However, the Required Actions for inoperable ECCS instrumentation channels provide appropriate compensatory measures for separate inoperable Condition entry for each inoperable ECCS instrumentation channel.

A.1

With one or more Functions with one required channel inoperable, one instrumentation channel must be restored to OPERABLE status, such that three required channels are OPERABLE. The 12-hour Completion Time is acceptable based on engineering judgment considering the reliability of the remaining OPERABLE channels and considering that most repairs will involve only card changes or sensor replacement. However, this out of service time is only acceptable provided the associated Function still maintains ECCS actuation capability (refer to Required Actions B.1 Bases).

BASES

ACTIONS (continued)

Alternatively, if it is not desired to restore the instrumentation channel to OPERABLE status, Condition B must be entered and its Required Action taken when the Completion Time of Required Action A.1 expires.

B.1

With the Required Action and associated Completion Time of Condition A not met or if multiple, inoperable, untripped channels (i.e., two or more required channels for most Functions) for the same Function result in the Function not maintaining ECCS actuation capability, the associated feature(s) may be incapable of performing the intended function and the affected ECCS components must be declared inoperable immediately. A Function is considered to be maintaining ECCS actuation capability when sufficient channels are OPERABLE or in trip such that the ECCS logic will generate a trip signal from the given Function on a valid signal.

SURVEILLANCE REQUIREMENTS

As noted at the beginning of the SRs, The SRs for each ECCS instrumentation Function are found in the SRs column of Table 3.3.5.1-1.

SR 3.3.5.1.1

Performance of the CHANNEL CHECK once every 12 hours ensures that a gross failure of instrumentation has not occurred.

The SSLC/ESF is cyclically tested from the sensor input point to the logic contact output by online self-diagnostics. The self-diagnostic capabilities include microprocessor checks, system initialization, watchdog timers, memory integrity checks, input/output (I/O) data integrity checks, communication bus interface checks, and checks on the application program (checksum).

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 match criteria, it may be an indication that the instrument has drifted outside its limit.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The Surveillance Frequency is based upon operating experience that demonstrates channel failure is rare. The CHANNEL CHECK every 12 hours supplements less formal, but more frequent checks of channels during normal operational use of the displays associated with the channels required by the LCO.

SR 3.3.5.1.2

A CHANNEL FUNCTIONAL TEST is performed on each required channel to ensure the entire channel will perform the intended function. This test ensures a complete CHANNEL FUNCTIONAL TEST of required instrument channels from the sensor input through the DTM function.

The SSLC/ESF is cyclically tested from the sensor input point to the logic contact output by online self-diagnostics. The self-diagnostic capabilities include microprocessor checks, system initialization, watchdog timers, memory integrity checks, input/output (I/O) data integrity checks, communication bus interface checks, and checks on the application program (checksum).

The Frequency of 31 days is based on the reliability of the ECCS instrumentation channels.

SR 3.3.5.1.3

A CHANNEL CALIBRATION is a complete check of the instrument loop and the sensor. This test verifies the required channel responds to the measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the required channel adjusted to the $NTSP_F$ within the "as-left" tolerance to account for instrument drifts between successive calibrations consistent with the methods and assumptions required by the SCP.

The Frequency is based upon the assumption of a 24-month calibration interval in the determination of the magnitude of equipment drift in the setpoint analysis.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.5.1.4

This SR ensures that the individual required channel response times are less than or equal to the maximum values assumed in the accident analysis. The ECCS RESPONSE TIME acceptance criteria are included in Reference 4.

ECCS RESPONSE TIME may be verified by actual response time measurements in any series of sequential, overlapping, or total channel measurements. This test encompasses the ECCS instrumentation from the input variable sensors through the DTM function. This test overlaps the testing required by SR 3.3.5.2.2 to ensure complete testing of instrument channels and actuation circuitry.

COL 16.0-1-A 3.3.5.1-2

[However, some sensors for Functions are allowed to be excluded from specific ECCS RESPONSE TIME measurement if the conditions of Reference XX are satisfied. If these conditions are satisfied, sensor response time may be allocated based on either assumed design sensor response time or the manufacturer's stated design response time. When the requirements of Reference XX are not satisfied, sensor response time must be measured. Furthermore, measurement of the instrument loops response times is not required if the conditions of Reference XX are satisfied.]

ECCS RESPONSE TIME tests are conducted on a 24 month STAGGERED TEST BASIS for three channels. The Frequency of 24 months on a STAGGERED TEST BASIS ensures that the required channels associated with each division are alternately tested.

The 24-month test Frequency is consistent with the typical industry refueling cycle and with operating experience that shows that random failures of instrumentation components causing serious response time degradation, but not channel failure, are infrequent.

BASES

REFERENCES	1.	Chapter 7.
	2.	Chapter 15.
	3.	Chapter 6.
	4.	Section 15.2.

B 3.3 INSTRUMENTATION

B 3.3.5.2 EMERGENCY CORE COOLING SYSTEM (ECCS) ACTUATION

BASES

BACKGROUND

The purpose of the ECCS actuation logic is to initiate appropriate responses from the ECCS to ensure that fuel is adequately cooled in the event of a design basis event.

The ECCS logic actuates the Automatic Depressurization System (ADS), the Gravity-Driven Cooling System (GDCS), the Isolation Condenser System, and Standby Liquid Control (SLC). The equipment involved with ADS is described in the Bases for LCO 3.5.1, “ADS - Operating.” The equipment involved with GDCS is described in the Bases for LCO 3.5.2, “Gravity-Driven Cooling System (GDCS) - Operating.” The equipment involved with SLC is described in the Bases for LCO 3.1.7, “Standby Liquid Control (SLC) System.”

A detailed description of the ECCS instrumentation and ECCS actuation logic is provided in the Bases for LCO 3.3.5.1, “Emergency Core Cooling System (ECCS) Instrumentation.”

This specification addresses OPERABILITY of the ECCS actuation circuitry from the outputs of the Digital Trip Module (DTM) functions through the voter logic unit (VLU) functions, the timers, and the load drivers (LDs) associated with the ADS safety relief valves (SRVs), the ADS depressurization valves (DPVs), the GDCS injection valves, the GDCS equalizing line valves, and the SLC squib-actuated valves. Operability requirements associated with the ECCS instrumentation channels are provided in LCO 3.3.5.1. Operability requirements for actuated components (i.e., squibs and solenoid valves) are addressed in LCO 3.1.7, LCO 3.5.1, and LCO 3.5.2, as appropriate.

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

The actions of the ECCS are explicitly assumed in the safety analyses of Reference 1 and 2. The ECCS is initiated to preserve the integrity of the fuel cladding by limiting the post-LOCA peak cladding temperature to less than the 10 CFR 50.46 limits.

ECCS Actuation satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

ECCS actuation supports OPERABILITY of the ECCS Instrumentation, “LCO 3.3.5.1, Emergency Core Cooling System (ECCS) Instrumentation” and therefore is required to be OPERABLE. This Specification addresses OPERABILITY of the ECCS actuation circuitry from the outputs of the DTM functions through the VLU functions, the timers, and the LDs associated with the ADS safety relief valves (SRVs), the ADS depressurization valves (DPVs), the GDCS injection valves, the GDCS equalizing line valves, and the SLC squib-actuated valves.

Although there are four divisions of ECCS actuation for each function, only three ECCS actuation divisions for each function are required to be OPERABLE. The three required divisions are those divisions associated with the DC and Uninterruptible AC Electrical Power Distribution Divisions required by LCO 3.8.6, "Distribution Systems - Operating," and LCO 3.8.7, "Distribution Systems - Shutdown." This is acceptable because the single-failure criterion is met with three OPERABLE ECCS actuation divisions, and because each ECCS actuation division is associated with and receives power from only one of the four electrical divisions.

1. Automatic Depressurization System (ADS)

The ADS actuation divisions receive input from the Reactor Vessel Level - Low, Level 1.0 signal sustained for 10 seconds, or from the Drywell Pressure - High signal sustained for 60 minutes. ADS actuation is required to be OPERABLE in MODES 1, 2, 3, and 4, consistent with the requirements of LCO 3.5.1, “Automatic Depressurization System (ADS) - Operating.” ADS actuation is required to be OPERABLE in MODE 5, and in MODE 6 prior to removal of the reactor pressure vessel head, consistent with the requirements of LCO 3.5.3, " Gravity-Driven Cooling System (GDCS) – Shutdown." Three actuation divisions are required to be OPERABLE to ensure that no single actuation failure can preclude the actuation function.

2. Gravity-Driven Cooling System (GDCS) Injection Lines

The GDCS injection line actuation divisions receive input from the Reactor Vessel Level - Low, Level 1.0 signal sustained for 10 seconds, or from the Drywell Pressure - High signal sustained for 60 minutes. GDCS injection line actuation is required to be OPERABLE in MODES 1, 2, 3, and 4, consistent with the requirements of LCO 3.5.2, “Gravity-Driven

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

Cooling System (GDCS) - Operating." GDCS injection line actuation is required to be OPERABLE in MODES 5 and 6, except with the buffer pool gate removed and water level ≥ 7.01 meters (23.0 feet) over the top of the reactor pressure vessel flange, consistent with the requirements of LCO 3.5.3, "Gravity-Driven Cooling System (GDCS) - Shutdown." Three actuation divisions are required to be OPERABLE to ensure that no single actuation failure can preclude the actuation function.

3. GDCS Equalizing Lines

The GDCS equalizing line actuation divisions receive input from the following instrumentation: Reactor Vessel Level - Low, Level 1.0 signal sustained for 10 seconds and Reactor Vessel Level - Low, Level 0.5. GDCS equalizing line actuation is required to be OPERABLE in MODES 1, 2, 3, and 4, consistent with the requirements of LCO 3.5.2, "Gravity-Driven Cooling System (GDCS) - Operating." GDCS equalizing line actuation is required to be OPERABLE in MODES 5 and 6, except with the buffer pool gate removed and water level ≥ 7.01 meters (23.0 feet) over the top of the reactor pressure vessel flange, consistent with the requirements of LCO 3.5.3, "Gravity-Driven Cooling System (GDCS) - Shutdown." Three actuation divisions are required to be OPERABLE to ensure that no single actuation failure can preclude that actuation function.

4. Standby Liquid Control (SLC)

The SLC actuation divisions receive inputs from the Reactor Vessel Level - Low, Level 1.0 signal sustained for 10 seconds. SLC actuation is required to be OPERABLE in MODES 1, 2, 3, and 4 consistent with the requirements of LCO 3.1.7, "Standby Liquid Control (SLC) System." Three actuation divisions are required to be OPERABLE to ensure that no single actuation failure can preclude that actuation function.

BASES

ACTIONS

A Note has been provided to modify the ACTIONS related to ECCS divisions of actuation logic. Section 1.3, Completion Times, specifies once a Condition has been entered, subsequent divisions, subsystems, components or variables expressed in the Condition discovered to be inoperable or not within limits, will not result in separate entry into the Condition. Section 1.3 also specifies Required Actions of the Condition continue to apply for each additional failure, with Completion Times based on initial entry into the Condition. However, the Required Actions for inoperable ECCS instrumentation channels provide appropriate compensatory measures for separate inoperable Condition entry for each inoperable division of ECCS actuation logic.

A.1

Condition A exists when one required ECCS actuation division is inoperable. In this Condition, ECCS actuation still maintains actuation trip capability, but cannot accommodate a single failure. The 12 hour Completion Time is acceptable based on engineering judgment considering the reliability of the remaining OPERABLE channels and considering that most repairs will involve only card changes or sensor replacement. However, this out of service time is only acceptable provided the associated Function still maintains ECCS actuation capability (refer to Required Actions B.1 Bases).

B.1

If the Required Actions and associated Completion Times of Condition A are not met or two or more required actuation divisions are inoperable, the affected actuation device(s) must be declared inoperable immediately. In this Condition, a loss of ECCS actuation capability occurs to numerous ECCS actuation devices. ECCS automatic actuation capability is considered to be maintained when sufficient actuation divisions are OPERABLE or in trip such that the ECCS logic will generate an actuation signal on a valid signal.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.3.5.2.1

The LOGIC SYSTEM FUNCTIONAL TEST demonstrates the OPERABILITY of the required ECCS logic for a specific division.

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 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 24 month Frequency.

SR 3.3.5.2.2

This SR ensures that the individual required division response times are less than or equal to the maximum values assumed in the accident analysis. The ECCS RESPONSE TIME acceptance criteria are included in Reference 3.

ECCS RESPONSE TIME may be verified by actual response time measurements in any series of sequential, overlapping, or total division measurements. This test encompasses the ECCS actuation circuitry from the outputs of the DTM functions through the VLU functions, the timers, and the LDs associated with the ADS SRVs, the ADS DPVs, the GDCS injection valves, the GDCS equalizing line valves, and the SLC squib-actuated valves. This test overlaps the testing required by SR 3.3.5.1.4 to ensure complete testing of instrument channels and actuation circuitry.

COL 16.0-1-A 3.3.5.2-1

[However, some portions of the ECCS actuation circuitry are allowed to be excluded from specific ECCS RESPONSE TIME measurement if the conditions of Reference XX are satisfied. Furthermore, measurement of the instrument loops response times is not required if the conditions of Reference XX are satisfied.]

ECCS RESPONSE TIME tests are conducted on a 24 month STAGGERED TEST BASIS for three divisions. The Frequency of 24 months on a STAGGERED TEST BASIS ensures that each required division is alternately tested.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The 24 month test Frequency is consistent with the typical industry refueling cycle and with operating experience that shows that random failures of instrumentation components causing serious response time degradation, but not channel failure, are infrequent.

REFERENCES

1. Chapter 15.
2. Chapter 6.
3. Section 15.2.

B 3.3 INSTRUMENTATION

B 3.3.5.3 Isolation Condenser System (ICS) Instrumentation

BASES

BACKGROUND

The purpose of the ICS instrumentation is to initiate appropriate actions to ensure ICS operates following a reactor pressure vessel (RPV) isolation after a scram to provide adequate RPV pressure reduction to preclude safety relief valve operation, conserve RPV water level to avoid automatic depressurization caused by low water level. In addition, in the event of a loss of coolant accident (LOCA), the ICS instrumentation ensures the system operates to provide liquid inventory to the RPV. The ICS instrumentation also ensures the ICS is vented to mitigate the accumulation of radiolytic hydrogen and oxygen in order to prevent a detonation. The equipment involved with ICS is described in the Bases for LCO 3.5.4, “Isolation Condenser System (ICS) - Operating.”

Technical Specifications are required by 10 CFR 50.36 to contain limiting safety system settings (LSSS) defined by the regulation as "...settings for automatic protective devices related to those variables having significant safety functions." Where LSSS is specified for a variable on which a Safety Limit (SL) has been placed, the setting must be chosen such that automatic protective action will correct the abnormal situation before a SL is exceeded. The Analytical Limit is the limit of the process variable at which a safety action is initiated, as established by the safety analysis, to ensure that a SL is not exceeded. Any automatic protection action that occurs on reaching the Analytical Limit therefore ensures that the SL is not exceeded. Where LSSS is specified for a variable having a significant safety function but which does not protect SLs, the setting must be chosen such that automatic protective actions will initiate consistent with the design basis. The Design Limit is the limit of the process variable at which a safety action is initiated to ensure that these automatic protective devices will perform their specified safety function.

The actual settings for automatic protective devices must be chosen to be more conservative than the Analytical / Design Limit to account for instrument loop uncertainties related to the setting at which the automatic protective action would actually occur. The methodology for determining the actual settings, and the required tolerances to maintain these settings conservative to the Analytical / Design Limits, including the requirements for determining that the channel is OPERABLE, are defined in the Setpoint Control Program (SCP), in accordance with Specification 5.5.11, "Setpoint Control Program (SCP)."

BASES

BACKGROUND (continued)

The Limiting Trip Setpoint (LTSP) is a predetermined setting for a protective device chosen to ensure automatic actuation prior to the process variable reaching the Analytical / Design Limit and thus ensuring that the SL would not be exceeded (i.e., for Analytical Limits), or that automatic protective actions occur consistent with the design basis (i.e., for Design Limits). As such, the LTSP accounts for process and primary element measurement errors, and uncertainties in setting the device (e.g., calibration), uncertainties in how the device might actually perform (e.g., accuracy), changes in the point of action of the device over time (e.g., drift during surveillance intervals), and any other factors that may influence its actual performance (e.g., harsh accident environments). In this manner, the LTSP ensures that SLs are not exceeded and that automatic protective devices will perform their specified safety function. As such, the LTSP meets the definition of an LSSS. The nominal trip setpoint to which the setpoint is reset after calibration is the $NTSP_F$, which is more conservative than the LTSP and has margin to assure that the Allowable Value is not exceeded during calibration.

Technical Specifications contain values related to the OPERABILITY of equipment required for safe operation of the facility. OPERABLE is defined in Technical Specifications as "...being capable of performing its safety function(s)." For automatic protective devices, the required safety function is to ensure that a SL is not exceeded and that automatic protective actions will initiate consistent with the design basis. Therefore, the LTSP is the LSSS as defined by 10 CFR 50.36. However, use of the LTSP to define OPERABILITY in Technical Specifications would be an overly restrictive requirement if it were applied as an OPERABILITY limit for the "as-found" value of a protective device setting during a Surveillance.

However, there is also some point beyond which the device would have not been able to perform its function due, for example, to greater than expected drift. This value is specified in the SCP, as required by Specification 5.5.11, in order to define OPERABILITY of the devices and is designated as the Allowable Value which is the least conservative value of the as-found setpoint that a channel can have during CHANNEL CALIBRATION. The LTSP, $NTSP_F$, Allowable Value, "as-found" tolerance, and "as-left" tolerance and the methodology for calculating the "as-left" and "as-found" tolerances will be maintained in the SCP, as required by Specification 5.5.11.

BASES

BACKGROUND (continued)

The Allowable Value is the least conservative value that the setpoint of the channel can have when tested such that a channel is OPERABLE if the setpoint is found conservative with respect to the Allowable Value during the CHANNEL CALIBRATION. Note that, although a channel is OPERABLE under these circumstances, the setpoint must be left adjusted to a value within the established "as-left" tolerance of the $NTSP_F$ and confirmed to be operating within the statistical allowances of the uncertainty terms assigned in the setpoint calculation. As such, the Allowable Value differs from the $NTSP_F$ by an amount equal to or greater than the "as-found" tolerance value. In this manner, the actual setting of the device will ensure that a SL is not exceeded or that automatic protective actions will initiate consistent with the design basis at any given point of time as long as the device has not drifted beyond that expected during the surveillance interval. If the actual setting of the device is found to be non-conservative with respect to the Allowable Value the device would be considered inoperable from a Technical Specification perspective. This requires corrective action including those actions required by 10 CFR 50.36 when automatic protective devices do not function as required.

The ICS can be automatically or manually initiated. The ICS actuates automatically in response to signals from any of the following:

1. Reactor Steam Dome Pressure - High for 10 seconds,
2. RPV Water Level - Low (Level 2), with time delay,
3. RPV Water Level - Low (Level 1),
4. Indication that two Main Steam Isolation Valves (MSIVs) in separate Main Steamlines (MSLs) are not fully open with the reactor mode switch in the run position, or
5. Loss of power generation buses.

ICS venting can be automatically or manually initiated. ICS venting actuates automatically, following a 6-hour time delay, in response to a signal that at least one Condensate Return Valve (i.e. the condensate return valve or the condensate return bypass valve) for a given ICS train has opened.

The Safety System Logic and Control Engineered Safety Features (SSLC/ESF) System controls the initiation signals and logic for ICS. SSLC/ESF is a four division, separated protection logic system designed to provide a very high degree of assurance to both ensure ICS initiation when required and prevent inadvertent initiation. The input and output

BASES

BACKGROUND (continued)

trip determinations for all ICS functions are based upon a two-out-of-four logic arrangement. Each division of SSLC/ESF is configured such that all functions (e.g., the digital trip module (DTM) function and voter logic unit (VLU) function) are implemented in triply redundant processors to support the requirement that single divisional failures cannot result in inadvertent actuation.

Four separate instrument channels are used to monitor ICS initiation parameters. Signals from sensors are multiplexed at the divisional level and the triply redundant sensor data is then transmitted to the SSLC/ESF triply redundant digital trip module (DTM) function for setpoint comparison. The output of each divisional DTM function (a trip/no-trip condition) is routed to all four divisional triply redundant VLU functions such that each divisional VLU function receives input from each of the four divisional DTM functions.

For maintenance purposes and added reliability, each DTM function has a division of sensors bypass such that all instruments in that division will be bypassed in the trip logic at the VLU functions. Thus, each VLU function will be making its trip decision on a two-out-of-three logic basis for each variable. It is possible for only one division of sensors bypass condition to be in effect at any time.

The processed trip signal from its own division and trip signals from the other three divisions are processed in the triply redundant VLU function for two-out-of-four voting.

The load driver arrangement for actuation of the ICS Condensate Return Valves are such that an actuation signal from two divisions of ICS actuation logic are required to actuate a condensate return flow path.

Equipment within a single division is powered from the safety-related power source of the same division.

This Specification provides Operability requirements for the ICS instrumentation from the input variable sensors through the DTM function. Operability requirements for the ICS actuation circuitry consisting of timers, VLU functions, and load drivers are provided by LCO 3.3.5.4, "Isolation Condenser System (ICS) Actuation." Operability requirements for the actuated components are addressed in LCO 3.5.4.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

The actions of the ICS are explicitly assumed in the safety analyses of Reference 1. The ICS is initiated to preserve the integrity of the fuel cladding by limiting the post-LOCA peak cladding temperature to less than the 10 CFR 50.46 limits. Actuation of the ICS precludes actuation of safety relief valves and limits the peak RPV pressure to less than the ASME Section III Code limits.

The ICS Instrumentation satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

The OPERABILITY of the ICS is dependent on the OPERABILITY of the individual instrumentation channel Functions specified in Table 3.3.5.3-1. Each Function must have the required number of OPERABLE channels, with their setpoints in accordance with the SCP, where appropriate. The actual setpoint is calibrated consistent with the SCP. Each channel must also respond within its assumed response time.

$NTSP_F$s are specified in the SCP, as required by Specification 5.5.11. The $NTSP_F$s are selected to ensure the actual setpoints are conservative with respect to the Allowable Value between successive CHANNEL CALIBRATIONS. Operation with a trip setpoint less conservative than the $NTSP_F$, but conservative with respect to its Allowable Value, is acceptable. A channel is inoperable if its actual trip setpoint is non-conservative with respect to its required Allowable Value.

The individual Functions are required to be OPERABLE in the MODES specified in the Table which may require an ICS actuation to mitigate the consequences of a design basis accident or transient.

Although there are four channels of ICS instrumentation for each function, only three ICS instrumentation channels for each function are required to be OPERABLE. The three required channels are those channels associated with the DC and Uninterruptible AC Electrical Power Distribution Divisions required by LCO 3.8.6, "Distribution Systems - Operating," and LCO 3.8.7, "Distribution Systems - Shutdown." This is acceptable because the single-failure criterion is met with three OPERABLE ICS instrumentation channels, and because each ICS instrumentation division is associated with and receives power from only one of the four electrical divisions.

The specific Applicable Safety Analyses, LCO and Applicability discussions are listed below on a Function-by-Function basis.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

1. Reactor Vessel Steam Dome Pressure - High

ICS is designed to operate following reactor pressure vessel (RPV) isolation to provide adequate RPV pressure reduction to preclude safety relief valve operation and provide core cooling while conserving reactor water inventory. Therefore, Reactor Vessel Steam Dome Pressure - High Function existing for 10 seconds initiates an ICS actuation for transients that result in a pressure increase. Actuation of the ICS provides RPV pressure reduction to preclude safety relief valve operation and provide core cooling.

High reactor pressure signals are initiated from four pressure sensors that sense reactor pressure. The Reactor Vessel Steam Dome Pressure - High Allowable Value provides a sufficient margin to the ASME Section III Code limits during the event.

Three channels of Reactor Vessel Steam Dome Pressure - High Function are required to be OPERABLE to ensure no single instrument failure will preclude ICS actuation.

The Function is required to be OPERABLE in MODES 1, 2, 3, 4, and 5 .

2. Reactor Vessel Water Level - Low, Level 2

Low reactor vessel water level indicates the capability to cool the fuel may be threatened. Should reactor vessel water level decrease too far, fuel damage could result. Therefore, an ICS actuation is initiated at Level 2, with a 30-second time delay to provide a source of core cooling. The time delay provides an allowance for temporary transients that may reduce RPV level below the Level 2 setpoint. This Function is assumed to be available to support the transient and design basis analyses (Ref. 1).

Reactor Vessel Water Level - Low, Level 2, signals are initiated from four wide range level sensors.

Three channels of Reactor Vessel Water Level Low, Level 2, Function are required to be OPERABLE to ensure no single instrument failure will prevent ICS actuation from this Function on a valid signal.

The Function is required to be OPERABLE in MODES 1, 2, 3, 4, and 5.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

3. Reactor Vessel Water Level - Low, Level 1

Low Reactor Vessel Water Level indicates the capability to cool the fuel may be threatened. Should RPV water level decrease too far, fuel damage could result. Therefore, ICS receives the signals necessary for initiation from this Function. The Reactor Vessel Water Level - Low, Level 1 is one of the Functions assumed to be OPERABLE and capable of actuating the ICS during the accidents analyzed in Reference 1. The core cooling function of the ICS along with the ECCS and the scram action of the RPS, assures that the fuel peak cladding temperature remains below the limits of 10 CFR 50.46.

Reactor Vessel Water Level - Low, Level 1 signals are initiated from four wide range level sensors.

Three channels of Reactor Vessel Water Level - Low, Level 1 Function are required to be OPERABLE when ICS is required to be OPERABLE to ensure that no single instrument failure can preclude ICS actuation, when required.

The Function is required to be OPERABLE in MODES 1, 2, 3, 4, and 5.

4. Main Steam Isolation Valve - Closure

Main Steam Isolation Valve (MSIV) closure results in loss of the main turbine and the condenser as a heat sink for the nuclear steam supply system and indicates a need to isolate the reactor to reduce excessive steam line flow or leakage outside the containment. Therefore, an ICS actuation is initiated on an MSIV closure signal before the MSIVs are completely closed in anticipation of the complete loss of the normal heat sink and subsequent overpressurization transient. MSIV closure is assumed in the transients and accidents analyzed in Reference 1. The ICS actuation, along with the reactor scram, assures that the fuel peak cladding temperature remains below the limits of 10 CFR 50.46.

The logic for the Main Steam Isolation Valve - Closure Function is arranged such that ICS initiation occurs if two MSIVs in separate MSLs are not fully open with the Reactor Mode Switch in run.

The MSIV - Closure Allowable Value is specified to ensure that an ICS initiation occurs prior to a significant reduction in steam flow, thereby reducing the severity of the subsequent pressure transient.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

Three channels of MSIV - Closure Function are required to be OPERABLE to ensure no single instrument failure will prevent the ICS actuation from this Function on a valid signal. This Function is only required in MODE 1 because with the MSIVs open and the heat generation rate high, a pressurization transient can occur if the MSIVs close.

5. Power Generation Bus Loss

The plant electrical system has four redundant power generation buses that operate at 13.8 kV. These buses supply power for the feedwater pumps and other pumps. In MODE 1, at least three of the four buses must be powered. The purpose of ICS initiation on losing feedwater flow is to provide a source of core cooling following the loss of feedwater pump function.

The Allowable Value was selected high enough to detect a loss of voltage in order to mitigate the reactor water level drop to Level 1 following the loss of feedwater pump function.

Three channels of Power Generation Bus Loss Function are required to be OPERABLE to ensure that no single instrument failure will prevent the ICS actuation from this Function on a valid signal. The Function is required in MODE 1 where considerable energy exists in the reactor coolant system resulting in the limiting transients and accidents. During MODES 2, 3, 4, 5, and 6, the core energy is significantly lower.

6. Condensate Return Valve – Open (per Isolation Condenser)

When an ICS initiation signals occurs, the condensate return valve and condensate return bypass valve for each ICS train open, which starts isolation condenser operation. After a six-hour time delay following either condensate return valve opening, the lower header vent valves automatically open to prevent the accumulation of radiolytically generated hydrogen and oxygen.

The logic for the Condensate Return Valve – Open Function is arranged such that the SSLC/ESF-actuated ICS vent valve will open upon opening of either of the condensate return valves on the associated ICS train.

Condensate Return Valve – Open signals are initiated from four position switches located on each condensate return and condensate return bypass valve.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

Three channels of the Condensate Return Valve - Open Function for each Condensate Return Valve on each ICS train are required to be OPERABLE when ICS is required to be OPERABLE to ensure that no single instrument failure can preclude ICS vent actuation, when required.

The Function is required to be OPERABLE in MODES 1, 2, 3, 4, and 5.

ACTIONS

The ACTIONS have been modified by a Note to permit separate Condition entry for each ICS instrumentation channel. Section 1.3, Completion Times, specifies once a Condition has been entered, subsequent divisions, subsystems, components or variables expressed in the Condition discovered to be inoperable or not within limits, will not result in separate entry into the Condition. Section 1.3 also specifies Required Actions of the Condition continue to apply for each additional failure, with Completion Times based on initial entry into the Condition. However, the Required Actions for inoperable ICS instrumentation channels provide appropriate compensatory measures for separate inoperable Condition entry for each inoperable ICS instrumentation channel.

<u>A.1</u>

With one or more Functions with one required channel inoperable, the affected required channel must be restored to OPERABLE status within 12 hours. The 12-hour Completion Time is acceptable based on engineering judgment considering the diversity of sensors available to provide actuation signals, the redundancy of the ICS instrumentation design, and the low probability of an event requiring ICS actuation during this period.

However, this out of service time is only acceptable provided the associated Function still maintains ICS actuation capability (refer to Required Actions B.1 Bases).

Alternatively, if the instrumentation channel can not be restored to OPERABLE status, Condition B must be entered and its Required Action taken when the Completion Time of Required Action A.1 expires.

BASES

ACTIONS (continued)

B.1

With the Required Action and associated Completion Time of Condition A not met or if multiple, untripped required channels (i.e., two or more required channels for most Functions) for the same Function result in the Function not maintaining ICS actuation capability, the associated feature(s) may be incapable of performing the intended function and the ICS trains must be declared inoperable immediately. A Function is considered to be maintaining ICS actuation capability when sufficient channels are OPERABLE or in trip such that the ICS logic will generate an initiation signal from the given Function on a valid signal.

SURVEILLANCE REQUIREMENTS

The Surveillance Requirements are modified by a Note. The Note directs the reader to Table 3.3.5.3-1 to determine the correct SRs to perform for each ICS Instrumentation Function.

SR 3.3.5.3.1

Performance of the CHANNEL CHECK once every 12 hours ensures that a gross failure of instrumentation has not occurred.

The SSLC/ESF is cyclically tested from the sensor input point to the logic contact output by online self-diagnostics. The self-diagnostic capabilities include microprocessor checks, system initialization, watchdog timers, memory integrity checks, input/output (I/O) data integrity checks, communication bus interface checks, and checks on the application program (checksum).

A CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

Agreement criteria are determined by the plant staff, based on a combination of the channel instrument uncertainties, including indication and readability. If a channel is outside the criteria, it may be an indication that the instrument has drifted outside its limit.

The Frequency is based upon operating experience that demonstrates channel failure is rare. The CHANNEL CHECK every 12 hours supplements less formal, but more frequent, checks of channels during normal operational use of the displays associated with the channels required by the LCO.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.5.3.2

A CHANNEL FUNCTIONAL TEST is performed on each required channel to ensure that the entire channel will perform the intended function. This test ensures a complete CHANNEL FUNCTIONAL TEST of required instrument channels from the sensor input through the DTM function.

The SSLC/ESF is cyclically tested from the sensor input point to the logic contact output by online self-diagnostics. The self-diagnostic capabilities include microprocessor checks, system initialization, watchdog timers, memory integrity checks, input/output (I/O) data integrity checks, communication bus interface checks, and checks on the application program (checksum).

The Frequency of 31 days is based on the reliability of the channels.

SR 3.3.5.3.3

A CHANNEL CALIBRATION is a complete check of the instrument loop and the sensor. This test verifies the required channel responds to the measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the required channel adjusted to the $NTSP_F$ within the "as-left" tolerance to account for instrument drifts between successive calibrations consistent with the methods and assumptions required by the SCP.

The Frequency is based upon the assumption of a 24 month calibration interval in the determination of the magnitude of equipment drift in the setpoint analysis.

SR 3.3.5.3.4

This SR ensures that the individual required channel response times are less than or equal to the maximum values assumed in the accident analysis. The ICS RESPONSE TIME acceptance criteria are included in Reference 2.

ICS RESPONSE TIME may be verified by actual response time measurements or any series of sequential, overlapping, or total channel measurements. This test encompasses the ICS instrumentation from the input variable sensors through the DTM function. This test overlaps the testing required by SR 3.3.5.4.2 to ensure complete testing of instrumentation channels and actuation circuitry.

BASES

SURVEILLANCE REQUIREMENTS (continued)

COL 16.0-1-A 3.3.5.3-2

[However, some sensors for Functions are allowed to be excluded from specific ICS RESPONSE TIME measurement if the conditions of Reference XX are satisfied. If these conditions are satisfied, sensor response time may be allocated based on either assumed design sensor response time or the manufacturer's stated design response time. When the requirements of Reference XX are not satisfied, sensor response time must be measured. Furthermore, measurement of the instrument loops response times is not required if the conditions of Reference XX are satisfied.]

ICS SYSTEM RESPONSE TIME tests are conducted on a 24-month STAGGERED TEST BASIS for three channels. The Frequency of 24 months on a STAGGERED TEST BASIS ensures that each required channel is alternately tested. The 24-month test Frequency is consistent with the typical refueling cycle and with operating experience that shows that random failures of instrumentation components causing serious response time degradation, but not channel failure, are infrequent.

REFERENCES

1. Chapter 15.
2. Section 15.2.

B 3.3 INSTRUMENTATION

B 3.3.5.4 Isolation Condenser System (ICS) Actuation

BASES

BACKGROUND	The purpose of the ICS actuation logic is to initiate appropriate actions to ensure ICS operates following a reactor pressure vessel (RPV) isolation after a scram to provide adequate RPV pressure reduction to preclude safety relief valve operation and to conserve RPV water level to avoid automatic depressurization caused by low water level. In addition, in the event of a loss of coolant accident (LOCA), the ICS instrumentation ensures the system operates to provide additional liquid inventory to the RPV upon opening of the condensate return valves. The ICS actuation logic also ensures the ICS is vented to mitigate the accumulation of radiolytic hydrogen and oxygen in order to prevent a detonation. A detailed description of the ICS actuation instrumentation is provided in the Bases for LCO 3.3.5.3, “Isolation Condenser System (ICS) Instrumentation.” This specification addresses OPERABILITY of the ICS actuation circuitry from the outputs of the Digital Trip Module (DTM) functions through the voter logic unit (VLU) functions, the timers and the load drivers (LDs) associated with the ICS. Operability requirements associated with ICS instrumentation channels are provided in LCO 3.3.5.3. Operability requirements for actuated components are addressed in LCO 3.5.4, "Isolation Condenser System (ICS) - Operating."
APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY	The actions of the ICS are explicitly assumed in the safety analyses of Reference 1. The ICS is initiated to preserve the integrity of the fuel cladding by limiting the post-LOCA peak cladding temperature to less than the 10 CFR 50.46 limits. Actuation of the ICS also, precludes actuation of safety relief valves and limits the peak RPV pressure to less than the ASME Section III Code limits. ICS actuation satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii). Although there are four divisions of ICS actuation, only three ICS actuation divisions for each function are required to be OPERABLE. The three required divisions are those divisions associated with the DC and Uninterruptible AC Electrical Power Distribution Divisions required by LCO 3.8.6, "Distribution Systems - Operating," and LCO 3.8.7, "Distribution Systems - Shutdown." This is acceptable because the

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

single-failure criterion is met with three OPERABLE ICS instrumentation divisions, and because each ICS instrumentation division is associated with and receives power from only one of the four electrical divisions.

1. ICS Initiation Actuation

The ICS Initiation Actuation logic is the logic associated with automatically placing the ICS into service.

The ICS Initiation Actuation divisions receive input from the following:

- Reactor Steam Dome Pressure - High for 10 seconds,
- RPV Water Level - Low (Level 2), with time delay,
- RPV Water Level - Low (Level 1),
- Indication that two Main Steam Isolation Valves (MSIVs) in separate Main Steamlines (MSLs) are not fully open with the reactor mode switch in the run position, or
- Loss of power generation buses.

The ICS Initiation Actuation is required to be OPERABLE in MODES 1, 2, 3, 4, and 5, to preclude actuation of safety relief valves and limit the peak RPV pressure to less than the ASME Section III Code limits. Additionally, ICS Initiation Actuation assists in preserving the integrity of the fuel cladding by limiting the post-LOCA peak cladding temperature to less than the 10 CFR 50.46 limits, and removing reactor decay heat following reactor shutdown and isolation.

2. ICS Vent Actuation

The ICS Vent Actuation divisions receive input from the Condensate Return Valve Position – Open signals for each Condensate Return Valve. The logic is arranged such that if either Condensate Return Valve is open for an ICS train, then its vent will open after a 6-hour time delay.

The ICS Vent Actuation is required to be OPERABLE in MODES 1,2,3,4, and 5 to support proper operation of the ICS and to mitigate the accumulation of radiolytic hydrogen and oxygen that could cause a detonation.

BASES

ACTIONS

A.1

Condition A exists when one required ICS actuation division is inoperable. In this Condition, ICS actuation still maintains actuation trip capability but can not accommodate a single failure. The 12-hour Completion Time is acceptable based on engineering judgment considering the diversity of sensors available to provide trip signals, the redundancy of the ICS actuation design, and the low probability of an event requiring ICS actuation during this period. However, this out of service time is only acceptable provided the associated Function still maintains ICS actuation capability (refer to Required Actions B.1 Bases).

B.1

With the Required Action and associated Completion Time of Condition A not met or if two or more required actuation divisions are inoperable, the affected ICS actuation device(s) must be declared inoperable immediately. ICS automatic actuation capability is considered to be maintained when sufficient actuation divisions are OPERABLE or in trip such that the ICS logic will generate an actuation signal on a valid signal.

SURVEILLANCE REQUIREMENTS

As noted at the beginning of the Surveillance Requirements, the SRs for each ICS Actuation Function are located in the SRs column of Table 3.3.5.4-1.

SR 3.3.5.4.1

The LOGIC SYSTEM FUNCTIONAL TEST demonstrates the OPERABILITY of the required ICS logic for a specific division.

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 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 24 month Frequency.

SR 3.3.5.4.2

This SR ensures that the individual required division response times are less than or equal to the maximum values assumed in the accident analysis. The ICS RESPONSE TIME acceptance criteria are included in Reference 2.

BASES

SURVEILLANCE REQUIREMENTS (continued)

ICS RESPONSE TIME may be verified by actual response time measurements in any series of sequential, overlapping, or total division measurements. This test encompasses the ICS actuation circuitry from the outputs of the DTM function through the VLU function, the timers and the LDs associated with the ICS. This test overlaps the testing required by SR 3.3.5.3.4 to ensure complete testing of instrument channels and actuation circuitry.

COL 16.0-1-A 3.3.5.4-1

[However, some portions of the ICS actuation circuitry are allowed to be excluded from specific ICS RESPONSE TIME measurement if the conditions of Reference XX are satisfied. Furthermore, measurement of the instrument loops response times is not required if the conditions of Reference XX are satisfied.]

ICS RESPONSE TIME tests are conducted on a 24 month STAGGERED TEST BASIS for three divisions. The Frequency of 24 months on a STAGGERED TEST BASIS ensures that each required division is alternately tested.

The 24-month test Frequency is consistent with the typical industry refueling cycle and with operating experience that shows that random failures of instrumentation components causing serious response time degradation, but not channel failure, are infrequent.

REFERENCES

1. Chapter 15.
2. Section 15.2.

B 3.3 INSTRUMENTATION

B 3.3.6.1 Main Steam Isolation Valve (MSIV) Instrumentation

BASES

BACKGROUND

The isolation instrumentation contained in this specification provides the capability to generate isolation signals to the MSIVs and main steamline (MSL) drain isolation valves. The function of the MSIVs and MSL drain isolation valves, in combination with other accident mitigation systems, is to limit fission product release during and following postulated Design Basis Accidents (DBAs).

Technical Specifications are required by 10 CFR 50.36 to contain limiting safety system settings (LSSS) defined by the regulation as "...settings for automatic protective devices related to those variables having significant safety functions." Where LSSS is specified for a variable on which a Safety Limit (SL) has been placed, the setting must be chosen such that automatic protective action will correct the abnormal situation before a SL is exceeded. The Analytical Limit is the limit of the process variable at which a safety action is initiated, as established by the safety analysis, to ensure that a SL is not exceeded. Any automatic protection action that occurs on reaching the Analytical Limit therefore ensures that the SL is not exceeded. Where LSSS is specified for a variable having a significant safety function but which does not protect SLs, the setting must be chosen such that automatic protective actions will initiate consistent with the design basis. The Design Limit is the limit of the process variable at which a safety action is initiated to ensure that these automatic protective devices will perform their specified safety function.

The actual settings for automatic protective devices must be chosen to be more conservative than the Analytical / Design Limit to account for instrument loop uncertainties related to the setting at which the automatic protective action would actually occur. The methodology for determining the actual settings, and the required tolerances to maintain these settings conservative to the Analytical / Design Limits, including the requirements for determining that the channel is OPERABLE, are defined in the Setpoint Control Program (SCP), in accordance with Specification 5.5.11, “Setpoint Control Program (SCP)."

The Limiting Trip Setpoint (LTSP) is a predetermined setting for a protective device chosen to ensure automatic actuation prior to the process variable reaching the Analytical / Design Limit and thus ensuring that the SL would not be exceeded (i.e., for Analytical Limits), or that automatic protective actions occur consistent with the design basis (i.e.,

BASES

BACKGROUND (continued)

for Design Limits). As such, the LTSP accounts for process and primary element measurement errors, and uncertainties in setting the device (e.g., calibration), uncertainties in how the device might actually perform (e.g., accuracy), changes in the point of action of the device over time (e.g., drift during surveillance intervals), and any other factors that may influence its actual performance (e.g., harsh accident environments). In this manner, the LTSP ensures that SLs are not exceeded and that automatic protective devices will perform their specified safety function. As such, the LTSP meets the definition of an LSSS. The nominal trip setpoint to which the setpoint is reset after calibration is the $NTSP_F$, which is more conservative than the LTSP and has margin to assure the Allowable Value is not exceeded during calibration.

Technical Specifications contain values related to the OPERABILITY of equipment required for safe operation of the facility. OPERABLE is defined in Technical Specifications as "...being capable of performing its safety function(s)." For automatic protective devices, the required safety function is to ensure that a SL is not exceeded and that automatic protective actions will initiate consistent with the design basis. Therefore, the LTSP is the LSSS as defined by 10 CFR 50.36. However, use of the LTSP to define OPERABILITY in Technical Specifications would be an overly restrictive requirement if it were applied as an OPERABILITY limit for the "as-found" value of a protective device setting during a Surveillance.

However, there is also some point beyond which the device would have not been able to perform its function due, for example, to greater than expected drift. This value is specified in the SCP, as required by Specification 5.5.11, in order to define OPERABILITY of the devices and is designated as the Allowable Value which is the least conservative value of the as-found setpoint that a channel can have during CHANNEL CALIBRATION. The LTSP, $NTSP_F$, Allowable Value, "as-found" tolerance, and "as-left" tolerance, and the methodology for calculating the "as-left" and "as-found" tolerances will be maintained in the SCP, as required by Specification 5.5.11.

The Allowable Value is the least conservative value that the setpoint of the channel can have when tested such that a channel is OPERABLE if the setpoint is found conservative with respect to the Allowable Value during the CHANNEL CALIBRATION. Note that, although a channel is OPERABLE under these circumstances, the setpoint must be left adjusted to a value within the established "as-left" tolerance of the $NTSP_F$ and confirmed to be operating within the statistical allowances of the

BASES

BACKGROUND (continued)

uncertainty terms assigned in the setpoint calculation. As such, the Allowable Value differs from the $NTSP_F$ by an amount equal to or greater than the "as-found" tolerance value. In this manner, the actual setting of the device will ensure that a SL is not exceeded or that automatic protective actions will initiate consistent with the design basis at any given point of time as long as the device has not drifted beyond that expected during the surveillance interval. If the actual setting of the device is found to be non-conservative with respect to the Allowable Value the device would be considered inoperable from a Technical Specification perspective. This requires corrective action including those actions required by 10 CFR 50.36 when automatic protective devices do not function as required.

The MSIV Isolation circuitry, as shown in Reference 1, is divided into four redundant divisions of sensor (instrument) channels, four trip logics, and the hard-wired MSIV solenoid logic circuitry. The MSIV Isolation circuitry is contained in the Reactor Trip and Isolation Function (RTIF) portion of the Safety-Related Distributed Control and Information System (Q-DCIS) along with the Reactor Protection System (RPS). Functional diversity is provided by monitoring a wide range of dependent and independent parameters. The input parameters to the MSIV logic are from instrumentation that monitors reactor vessel water level (Level 1 and Level 2), main steam line pressure, main steam line flow, condenser pressure, main steam tunnel ambient temperature, and main steam turbine area ambient temperature. The plant parameters that are required to be monitored for MSIV logic are each measured independently by four sensors. Each sensor is assigned to one of the four redundant instrument channels, which are in turn associated with four divisions of logic. For any monitored parameter, the sensor signals of at least two of the four redundant instrument channels must exceed a predetermined setpoint value for trip to occur in a division of logic.

Each MSIV Isolation division has a Remote Multiplexer Unit (RMU) function, a Digital Trip Module (DTM) function, a Trip Logic Unit (TLU) function, and the Output Logic Unit (OLU) function. The RMU receives input from the sensor devices and performs analog-to-digital conversion and signal processing functions. The digitized signal is then sent to the DTM. The DTM generates the trip signal based on setpoint comparison. Each DTM sends a separate trip/no trip output signal to the TLUs in the four divisions of trip logic. Each TLU performs the two-out-of-four logic function to determine the trip status for each of the four divisions.

BASES

BACKGROUND (continued)

For maintenance purposes and added reliability, each TLU receives a division of sensors bypass such that all instruments in that division can be bypassed in the trip logic at the TLU. Thus, each TLU will be making its trip decision on a two-out-of-three logic basis for each variable. It is possible for only one division of sensors bypass condition to be in effect at any time.

The two-out-of-four trip logic decision (or two-out-of-three if a division of sensors bypass is in effect) is made by each TLU on a per variable basis such that setpoint exceedence in two instrument divisions for the same variable is required to initiate a trip output at the TLU. Since each TLU sees the outputs from all four DTMs, all four divisions of logic should sense and initiate a required trip simultaneously. A two-out-of-four trip in a TLU causes a trip in its corresponding OLU. It is this trip that then initiates an isolation by tripping load drivers in the power circuits that energize the MSIV solenoids. Each OLU sends output signals to load drivers associated with the MSIV solenoids and MSL drain isolation valves. The overall arrangement of OLU outputs and load driver groupings is such that a trip of any two of four TLUs (and associated OLUs) will result in full isolation of all MSLs. Each of the four TLUs has a division of logic bypass switch so that they can be bypassed, only one at any one time, such that the MSIV output logic reverts to two-out-of-three, i.e., the tripping of any two of the three remaining TLUs will still result in a full MSIV isolation. However, with this bypass in effect, the OLU for the division can be manually actuated at the OLU. Each OLU has test and trip switches such that the load drivers can be tested both with and without causing a full isolation condition.

Equipment within a single division is powered from the safety-related power source of the same division.

This Specification provides the OPERABILITY requirements for the MSIV isolation instrumentation from the input variable sensors through the DTM digital trip function. Operability requirements for the MSIV isolation actuation circuitry consisting of the TLU two-out-of-four function, timers, OLUs, and load drivers are provided by LCO 3.3.6.2, "Main Steam Isolation Valve (MSIV) Actuation." Operability requirements for actuated components (i.e., MSIV solenoid valves) are addressed in LCO 3.6.1.3, "Containment Isolation Valves (CIVs)."

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

The isolation signals generated by the MSIV instrumentation are assumed in the safety analyses of References 2 and 3 to initiate closure of the MSIVs and MSL drain isolation valves to limit offsite doses. Refer to LCO 3.6.1.3, "Containment Isolation Valves (CIVs)," Applicable Safety Analyses Bases, for more detail on MSIV isolation.

MSIV isolation instrumentation satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii). However, certain monitored instrumentation parameters are retained for other reasons and are described below in the individual process parameter discussion.

The OPERABILITY of the MSIV isolation instrumentation is dependent on the OPERABILITY of the individual instrumentation channel Functions specified in Table 3.3.6.1-1. Each Function must have the required number of OPERABLE channels, with their setpoints in accordance with the SCP, where appropriate. Each channel must also respond within its assumed response time, where appropriate.

$NTSP_F$s are specified in the SCP, as required by Specification 5.5.11. The $NTSP_F$s are selected to ensure the setpoints are conservative with respect to the Allowable Value between successive CHANNEL CALIBRATIONS. Operation with a trip setpoint less conservative than the $NTSP_F$, but conservative with respect to its Allowable Value, is acceptable. A channel is inoperable if its actual trip setpoint is non-conservative with respect to its required Allowable Value.

In general, the individual monitored process parameters are required to be OPERABLE in MODES 1, 2, 3, and 4 consistent with the Applicability of LCO 3.6.1.3. Functions that have different Applicabilities are discussed below in the individual Functions discussion.

Although there are four channels of MSIV instrumentation for each function, only three channels of MSIV instrumentation for each function are required to be OPERABLE. The three required channels are those channels associated with the DC and Uninterruptible AC Electrical Power Distribution Divisions required by LCO 3.8.6, "Distribution Systems - Operating." This is acceptable because the single-failure criterion is met with three OPERABLE MSIV instrumentation channels, and because each MSIV instrumentation division is associated with and receives power from only one of the four electrical divisions.

The specific Applicable Safety Analyses, LCO and specific Applicability discussions are provided below on a Function basis.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

1. Reactor Vessel Water Level - Low, Level 2

Low reactor pressure vessel (RPV) water level indicates the capability to cool the fuel may be threatened. Should RPV water level decrease too far, fuel damage could result. The isolations of the MSIVs and MSL drain isolation valves limit the release of fission products to help ensure that offsite does limits are not exceeded. The Reactor Vessel Water Level - Low, Level 2 is explicitly credited in the LOCA inside containment radiological analysis (Ref. 4)

Reactor Vessel Water Level - Low, Level 2 signals are initiated from four level sensors that sense the difference between the pressure due to a constant column (reference leg) of water and the pressure due to the actual water level (variable leg) in the vessel. Three channels of Reactor Vessel Water Level - Low, Level 2 Function are required to be OPERABLE to ensure no single instrument failure can preclude the isolation function.

The Reactor Vessel Water Level - Low, Level 2 Allowable Value was chosen to be the same as the Isolation Condenser System Reactor Vessel Water Level - Low, Level 2 Allowable Value.

2. Reactor Vessel Water Level - Low, Level 1

Low RPV water level indicates the capability to cool the fuel may be threatened. Should RPV water level decrease too far, fuel damage could result. The isolations of the MSIVs and MSL drain isolation valves limit the release of fission products to help ensure that offsite does limits are not exceeded. The Reactor Vessel Water Level - Low, Level 1 channels are provided as a backup to the Reactor Vessel Water Level - Low, Level 2 channels and are not credited in the safety analysis.

Reactor Vessel Water Level - Low, Level 1 signals are initiated from four level sensors that sense the difference between the pressure due to a constant column (reference leg) of water and the pressure due to the actual water level (variable leg) in the vessel. Three channels of Reactor Vessel Water Level - Low, Level 1 Function are required to be OPERABLE to ensure no single instrument failure can preclude the isolation function.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

The Reactor Vessel Water Level - Low, Level 1 Allowable Value was chosen to be the same as the Automatic Depressurization Reactor Vessel Water Level - Low, Level 1 Allowable Value.

3. Main Steam Line Pressure - Low

Low main steam line pressure indicates that there may be a problem with the turbine pressure regulation that could result in the Reactor Pressure Vessel (RPV) cooling down more than 55.6°C/hr (100°F/hr) if the pressure loss is allowed to continue. The Main Steam Line Pressure - Low Function is directly assumed in the analysis of the pressure regulator failure (Ref. 5). For this event the closure of the MSIVs and MSL drain isolation valves ensures that the RPV temperature change limit of 55.6°C/hr (100°F/hr) is not reached.

The main steam line low-pressure signals are initiated from four sensors that sense the pressure downstream of the outboard MSIVs. The sensors are arranged such that, even though physically separated from each other, each sensor is able to detect low main steam line pressure. Three channels of Main Steam Line Pressure - Low Function are required to be OPERABLE to ensure no single instrument failure can preclude the isolation function. The Allowable Value was selected to be high enough to prevent excessive RPV depressurization.

The Main Steam Line Pressure - Low Function is only required to be OPERABLE in MODE 1 since this is when the assumed transient can occur (Ref. 5).

4. Main Steam Line Flow - High (per Steam Line)

Main Steam Line Flow - High is provided to detect a break of the main steam line (MSL) and to initiate closure of the MSIVs and MSL drain isolation valves. If the steam were allowed to continue flowing out the break, the reactor would depressurize and the core could uncover. If the RPV water level decreases too far, fuel damage could occur. Therefore, the isolation is initiated on high flow to prevent or minimize core damage. The Main Steam Line Flow - High Function is directly assumed in the analysis of the MSL break (Ref. 6). The isolation action, along with the scram function of the RPS and the operation of the ECCS and Safety Relief Valves assures that the fuel peak cladding temperature remains below the limits of 10 CFR 50.46 and offsite dose limits.

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

The MSL flow signals are initiated from 16 differential pressure sensors that are connected to the four MSLs, four per steam line. The differential pressure sensors are arranged such that, even though physically separated from each other, all four connected to one MSL would be able to detect the high flow in that steam line. High MSL flow in any steam line will result in isolation of all MSLs. Three channels of Main Steam Line Flow - High Function for each main steam line are required to be OPERABLE so that no single instrument failure will preclude detecting a break in any individual main steam line.

The Allowable Value is chosen to ensure that offsite dose limits are not exceeded due to the break.

5. Condenser Pressure - High (per condenser)

The Condenser Pressure - High Function is provided to prevent overpressurization of the main condenser in the event of a loss of main condenser vacuum. Since the integrity of the condenser is an assumption in offsite dose calculations, the Condenser Pressure - High Function is assumed to be OPERABLE and capable of initiating closure of the MSIVs. The closure of the MSIVs and MSL drain isolation valves is initiated to prevent the addition of steam that would lead to additional condenser pressurization and possible rupture of the diaphragm installed to protect the turbine exhaust hood, thereby preventing a potential radiation leakage path following an accident. The Condenser Pressure - High Function is credited in the transients in References 7 and 8.

Condenser pressure signals are derived from four pressure sensors that sense the pressure in the condenser. Three channels of Condenser Pressure - High Function (per condenser) are required to be OPERABLE to ensure no single instrument failure can preclude the isolation function.

The Allowable Value is chosen to prevent damage to the condenser due to pressurization, thereby ensuring its integrity for offsite dose analysis.

The Condenser Pressure – High Function is required to be OPERABLE in MODE 1. This Function is bypassed when the Reactor Mode Switch is not in the Run position.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

6, 7. Main Steam Tunnel and Turbine Area Ambient Temperature - High

Main Steam Tunnel and Turbine Area Ambient Temperature - High Functions are provided to detect a leak in the reactor coolant pressure boundary and provide diversity to the MSL high flow instrumentation. The isolation occurs when a very small leak has occurred. If the small leak is allowed to continue without isolation, offsite dose limits may be reached. However, credit for these instruments is not taken in any transient or accident analysis because bounding analyses are performed for large breaks such as a MSL break.

Ambient temperature signals are initiated from thermocouples located away from the main steam lines so they are only sensitive to ambient air temperature. Three channels of Main Steam Tunnel Temperature - High Function are available and required to be OPERABLE to ensure no single instrument failure can preclude the isolation function. Three channels of Turbine Area Ambient Temperature - High Function are required to be OPERABLE to ensure no single instrument failure can preclude the isolation function.

The ambient temperature monitoring Allowable Value is based on the room or compartment size and the cooling provisions of the ventilation system.

ACTIONS

A Note has been provided to modify the ACTIONS related to Isolation Instrumentation channels. Section 1.3, Completion Times, specifies once a Condition has been entered, subsequent divisions, subsystems, components or variables expressed in the Condition discovered to be inoperable or not within limits, will not result in separate entry into the Condition. Section 1.3 also specifies Required Actions of the Condition continue to apply for each additional failure, with Completion Times based on initial entry into the Condition. However, the Required Actions for inoperable MSIV Instrumentation channels provide appropriate compensatory measures for separate inoperable channels. As such, a Note has been provided which allows separate Condition entry for each inoperable MSIV Instrumentation channel.

A.1

The 12-hour Completion Time is acceptable based on engineering judgment considering the diversity of sensors available to provide isolation signals, the redundancy of the MSIV isolation design, and the

BASES

ACTIONS (continued)

low probability of an event requiring an MSIV isolation during this interval. However, this out of service time is only acceptable provided the associated Function still maintains MSIV isolation capability (refer to Required Action B.1 Bases). If the inoperable channel cannot be restored to OPERABLE status within the 12-hour Completion Time, the associated instrument channel must be verified to be in trip. This is acceptable because verifying the associated instrument channel in trip conservatively compensates for the inoperability by placing the MSIV isolation instrumentation in a one-out-of-two configuration, restoring the capability to accommodate a single failure.

Alternatively, if it is not desirable to verify the associated instrument channel in trip (as in the case where it is desired to place the affected channel of sensors in bypass), Condition C must be entered and its Required Action taken when the Completion Time of Required Action A.1 expires.

<u>B.1</u>

Required Action B.1 directs entry into the appropriate Condition referenced in Table 3.3.6.1-1 if the Required Action and Completion Time of Condition A is not met or if multiple, inoperable, untripped required channels (i.e., two or more required channels) for the same Function result in the Function not maintaining isolation capability. A Function is considered to be maintaining MSIV isolation capability when sufficient channels are OPERABLE or in trip such that the MSIV isolation logic will generate a trip signal from the given Function on a valid signal to at least one valve in the associated penetration flow path. The applicable Condition specified in the Table is Function and MODE or other specified condition dependent.

<u>C.1</u>

If the required channel(s) is not restored to OPERABLE status, or verified to be in trip within the allowed Completion Time, or if MSIV isolation capability is not maintained, the plant must be placed in a MODE or other specified condition in which the LCO does not apply. This is done by placing the plant in at least MODE 2 within 6 hours.

The allowed Completion Time of 6 hours is reasonable, based on operating experience, to reach MODE 2 from full power conditions in an orderly manner and without challenging plant systems.

BASES

ACTIONS (continued)

D.1

If the required channel(s) is not restored to OPERABLE status, or verified to be in trip within the allowed Completion Time, or if MSIV isolation capability is not maintained, plant operations may continue if the associated MSIV(s) and MSL drain isolation valve(s) are declared inoperable. Because this Function is required to ensure that the MSIVs and MSL drain isolation valves perform their intended function, sufficient remedial measures are provided by declaring the associated MSIV(s) and MSL drain isolation valves inoperable immediately.

SURVEILLANCE REQUIREMENTS

As noted at the beginning of the Surveillance Requirements, the SRs for each isolation instrumentation Function are located in the SRs column of Table 3.3.6.1-1.

SR 3.3.6.1.1

Performance of the CHANNEL CHECK once every 12 hours ensures that a gross failure of instrumentation has not occurred.

The RTIF is cyclically tested from the sensor input point to the logic contact output by online self-diagnostics. The self-diagnostic capabilities include microprocessor checks, system initialization, watchdog timers, memory integrity checks, input/output (I/O) data integrity checks, communication bus interface checks, and checks on the application program (checksum).

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 unit staff, based on a combination of the channel instrument uncertainties, including indication, and readability. If a channel is outside the match criteria, it may be an indication that the instrument has drifted outside its limit.

The Surveillance Frequency is based on operating experience that demonstrates channel failure is rare.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The CHANNEL CHECK supplements less formal, but more frequent checks of channels during normal operational use of the displays associated with the LCO required channels.

SR 3.3.6.1.2

A CHANNEL FUNCTIONAL TEST is performed on each required channel to ensure that the channel will perform the intended function. This test ensures a complete CHANNEL FUNCTIONAL TEST of required instrument channels from the sensor input through the DTM function.

The RTIF is cyclically tested from the sensor input point to the logic contact output by online self-diagnostics. The self-diagnostic capabilities include microprocessor checks, system initialization, watchdog timers, memory integrity checks, input/output (I/O) data integrity checks, communication bus interface checks, and checks on the application program (checksum).

The Frequency of 31 days is based on the reliability of the Isolation Instrumentation channels.

SR 3.3.6.1.3

CHANNEL CALIBRATION is a complete check of the instrument loop and the sensor. This test verifies that the required channel responds to the measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the required channel adjusted to the $NTSP_F$ within the "as-left" tolerance to account for instrument drifts between successive calibrations consistent with the methods and assumptions required by the SCP.

The Surveillance Frequency is based upon the assumption of a 24-month calibration interval in the determination of the magnitude of equipment drift in the setpoint analysis.

SR 3.3.6.1.4

This SR ensures that the individual required channel response times are less than or equal to the maximum values assumed in the accident analysis. The instrument response times must be added to the associated closure times to obtain the ISOLATION SYSTEM RESPONSE

BASES

SURVEILLANCE REQUIREMENTS (continued)

TIME. ISOLATION SYSTEM RESPONSE TIME acceptance criteria are included in Reference 9. ISOLATION SYSTEM RESPONSE TIME may be verified by actual response time measurements in any series of sequential, overlapping, or total channel measurements. This test encompasses the MSIV isolation instrumentation from the input variable sensors through the DTM digital trip function. This test overlaps the testing required by SR 3.3.6.2.2 to ensure complete testing of instrumentation channels and actuation circuitry.

COL 16.0-1-A 3.3.6.1-2

[However, some sensors are allowed to be excluded from specific ISOLATION SYSTEM RESPONSE TIME measurement if the conditions of Reference XX are satisfied. If these conditions are satisfied, sensor response time may be allocated based on either assumed design sensor response time or the manufacturer's stated design response time. When the requirements of Reference XX are not satisfied, sensor response time must be measured. Furthermore, measurement of the instrument loops response time for some Functions is not required if the conditions of Reference XX are satisfied.]

ISOLATION SYSTEM RESPONSE TIME tests are conducted on a 24-month STAGGERED TEST BASIS for three channels. The Frequency of 24 months on a STAGGERED TEST BASIS ensures that the channels associated with each required division are alternately tested. The 24-month test Frequency is consistent with the refueling cycle and with operating experience that shows that random failures of instrumentation components causing serious response time degradation, but not channel failure, are infrequent.

REFERENCES

1. Chapter 7, Figure 7.2-1.
2. Section 6.2.
3. Chapter 15.
4. Subsection 15.4.4.
5. Subsection 15.3.3.
6. Subsection 15.4.5.

BASES

REFERENCES (continued)

7. Subsection 15.2.5.2.

8. Subsection 15.2.2.8.

9. Section 15.2.

B 3.3 INSTRUMENTATION

B 3.3.6.2 Main Steam Isolation Valve (MSIV) Actuation

BASES

BACKGROUND	The MSIV actuation logic is designed to isolate the MSIVs and Main Steamline (MSL) drain isolation valves when one or more monitored parameters exceed the specified limit. The function of the MSIVs and MSL drain isolation valves, in combination with other accident mitigation systems, is to limit fission product release during postulated Design Basis Accidents (DBAs). MSIV and MSL drain isolation valve isolation within the times specified ensure that the release of radioactive materials to the environment will be consistent with the assumptions used in the analysis of DBAs. A detailed description of the MSIV instrumentation and MSIV actuation logic is provided in the Bases for LCO 3.3.6.1, "Main Steam Isolation Valve (MSIV) Instrumentation." This Specification provides requirements for the MSIV actuation circuitry consisting of the inputs to the Trip Logic Units (TLUs) through the Output Logic Units (OLUs) through the Load Drivers (LDs), and the associated timers. Operability of the MSIV instrumentation channels, up to and including the digital trip function of the Digital Trip module (DTM), is addressed by LCO 3.3.6.1. The OPERABILITY of the MSIVs, MSL drain isolation valves and their associated solenoids is addressed by LCO 3.6.1.3, "Containment Isolation Valves (CIVs)."
APPLICABLE SAFETY ANALYSES	The isolation signals generated by the MSIV instrumentation are assumed in the safety analyses of References 1 and 2 to initiate closure of the MSIVs and MSL drain isolation valves to limit offsite doses. Refer to LCO 3.6.1.3, "Containment Isolation Valves (CIVs)," Applicable Safety Analyses Bases, for more detail on MSIVs and MSL drain isolation valves. MSIV Actuation satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).
LCO	Although there are four MSIV actuation divisions, only three are required to be OPERABLE to ensure no single automatic actuation division failure will preclude an MSIV isolation to occur on a valid signal. The three required divisions are those divisions associated with the DC and Uninterruptible AC Electrical Power Distribution Divisions required by

BASES

LCO (continued)

LCO 3.8.6, "Distribution Systems - Operating." This is acceptable because the single-failure criterion is still met with three OPERABLE MSIV actuation divisions, and because each MSIV division is associated with and receives power from only one of the four electrical divisions.

APPLICABILITY

The MSIV actuation divisions are required to be OPERABLE in MODES 1, 2, 3, and 4 consistent with the Applicability of LCO 3.3.6.1 and LCO 3.6.1.3.

ACTIONS

A Note has been provided to modify the ACTIONS related to MSIV actuation divisions. Section 1.3, Completion Times, specifies once a Condition has been entered, subsequent divisions, subsystems, components or variables expressed in the Condition discovered to be inoperable or not within limits, will not result in separate entry into the Condition. Section 1.3 also specifies Required Actions of the Condition continue to apply for each additional failure, with Completion Times based on initial entry into the Condition. However, the Required Actions for inoperable MSIV actuation divisions provide appropriate compensatory measures for separate inoperable divisions. As such, a Note has been provided which allows separate Condition entry for each inoperable MSIV actuation division.

A.1

The 12-hour Completion Time is acceptable based on engineering judgment considering the diversity of sensors available to provide isolation signals, the redundancy of the MSIV isolation design, and the low probability of an event requiring an MSIV isolation during this interval. However, this out of service time is only acceptable provided the associated Function still maintains MSIV actuation capability (refer to Required Actions B.1 Bases). If the inoperable required division cannot be restored to OPERABLE status within the 12-hour Completion Time, the affected actuation division must be verified to be in trip. This is acceptable because verifying the affected MSIV isolation actuation division in trip conservatively compensates for the inoperability by placing the MSIV isolation actuation in a one-out-of-two configuration, restoring the capability to accommodate a single failure.

BASES

ACTIONS (continued)

Alternatively, if it is not desirable to verify the affected required actuation division in trip (as in the case where it is desired to place the affected division in bypass), Condition C must be entered and its Required Action taken when the Completion Time of Required Action A.1 expires.

B.1

If the Required Actions and associated Completion Times of Condition A are not met or two or more required MSIV actuation divisions are inoperable, the affected actuation device(s) must be declared inoperable immediately. In this Condition, a loss of MSIV actuation capability occurs to numerous actuation devices. MSIV actuation capability is considered to be maintained when sufficient required actuation divisions will generate an isolation from a given Function on a valid signal so that at least one valve in the associated penetration flow path is isolated.

SURVEILLANCE REQUIREMENTS

SR 3.3.6.2.1

The LOGIC SYSTEM FUNCTIONAL TEST demonstrates the OPERABILITY of the MSIV actuation divisions, including the two-out-of-four function of the Trip Logic Unit (TLU), Output Logic Unit (OLU), and Load Drivers (LDs) for a specific division. The testing in LCO 3.3.6.1 and LCO 3.6.1.3 overlaps this Surveillance to provide complete testing of the assumed safety function.

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 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 24-month Frequency.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.6.2.2

This SR ensures that the individual required division response times are less than or equal to the maximum values assumed in the accident analysis. The instrument response times must be added to the associated closure times to obtain the ISOLATION SYSTEM RESPONSE TIME. ISOLATION SYSTEM RESPONSE TIME acceptance criteria are included in Reference 3. ISOLATION SYSTEM RESPONSE TIME may be verified by actual response time measurements in any series of sequential, overlapping, or total channel measurements. This test encompasses the MSIV actuation circuitry consisting of the inputs to the TLUs through the OLUs through the LDs, and the associated timers. This test overlaps the testing required by SR 3.3.6.1.4 to ensure complete testing of instrumentation channels and actuation circuitry.

COL 16.0-1-A 3.3.6.2-1

[However, some portions of the MSIV actuation circuitry are allowed to be excluded from specific ISOLATION SYSTEM RESPONSE TIME measurement if the conditions of Reference XX are satisfied. Furthermore, measurement of the instrument loops response times is not required if the conditions of Reference XX are satisfied.]

ISOLATION SYSTEM RESPONSE TIME tests are conducted on a 24 month STAGGERED TEST BASIS for three divisions. The Frequency of 24 months on a STAGGERED TEST BASIS ensures that the channels associated with each required division are alternately tested. The 24-month test Frequency is consistent with the refueling cycle and with operating experience that shows that random failures of instrumentation components causing serious response time degradation, but not channel failure, are infrequent.

REFERENCES

1. Section 6.2.

2. Chapter 15.

3. Section 15.2.

B 3.3 INSTRUMENTATION

B 3.3.6.3 Isolation Instrumentation

BASES

BACKGROUND

The isolation instrumentation contained in this specification provides the capability to generate isolation signals to the containment isolation valves, the reactor building heating, ventilation and air conditioning system isolation dampers, and feedwater isolation valves. The function of the isolation valves and dampers, in combination with other accident mitigation systems, is to limit fission product release during and following postulated Design Basis Accidents (DBAs). The function of the feedwater isolation valves is to also limit the mass addition of water into containment during and following a design basis feedwater line rupture inside containment. The function of the reactor water cleanup/shutdown cooling (RWCU/SDC) isolation valves in MODES 5 and 6 is to protect the core by isolating the RWCU/SDC system from the reactor pressure vessel and minimizing a potential loss of coolant resulting from a line break in the RWCU/SDC system. The function of high pressure control rod drive (HP CRD) makeup water injection isolation is to prevent the long-term addition of inventory into containment following a loss of coolant accident (LOCA). The function of the ICS isolation that occurs when 2 or more Depressurization Valves (DPVs) are open is to mitigate the accumulation of radiolytic hydrogen and oxygen that could result in a detonation.

Technical Specifications are required by 10 CFR 50.36 to contain limiting safety system settings (LSSS) defined by the regulation as "...settings for automatic protective devices related to those variables having significant safety functions." Where LSSS is specified for a variable on which a Safety Limit (SL) has been placed, the setting must be chosen such that automatic protective action will correct the abnormal situation before a SL is exceeded. The Analytical Limit is the limit of the process variable at which a safety action is initiated, as established by the safety analysis, to ensure that a SL is not exceeded. Any automatic protection action that occurs on reaching the Analytical Limit therefore ensures that the SL is not exceeded. Where LSSS is specified for a variable having a significant safety function but which does not protect SLs, the setting must be chosen such that automatic protective actions will initiate consistent with the design basis. The Design Limit is the limit of the process variable at which a safety action is initiated to ensure that these automatic protective devices will perform their specified safety function.

BACKGROUND (continued)

The actual settings for automatic protective devices must be chosen to be more conservative than the Analytical / Design Limit to account for instrument loop uncertainties related to the setting at which the automatic protective action would actually occur. The methodology for determining the actual settings, and the required tolerances to maintain these settings conservative to the Analytical / Design Limits, including the requirements for determining that the channel is OPERABLE, are defined in the Setpoint Control Program (SCP), in accordance with Specification 5.5.11, “Setpoint Control Program (SCP)."

The Limiting Trip Setpoint (LTSP) is a predetermined setting for a protective device chosen to ensure automatic actuation prior to the process variable reaching the Analytical / Design Limit and thus ensuring that the SL would not be exceeded (i.e., for Analytical Limits), or that automatic protective actions occur consistent with the design basis (i.e., for Design Limits). As such, the LTSP accounts for process and primary element measurement errors, and uncertainties in setting the device (e.g., calibration), uncertainties in how the device might actually perform (e.g., accuracy), changes in the point of action of the device over time (e.g., drift during surveillance intervals), and any other factors that may influence its actual performance (e.g., harsh accident environments). In this manner, the LTSP ensures that SLs are not exceeded and that automatic protective devices will perform their specified safety function. As such, the LTSP meets the definition of an LSSS. The nominal trip setpoint to which the setpoint is reset after calibration is the $NTSP_F$, which is more conservative than the LTSP and has margin to assure that the Allowable Value is not exceeded during calibration.

Technical Specifications contain values related to the OPERABILITY of equipment required for safe operation of the facility. OPERABLE is defined in Technical Specifications as "...being capable of performing its safety function(s)." For automatic protective devices, the required safety function is to ensure that a SL is not exceeded and that automatic protective actions will initiate consistent with the design basis. Therefore, the LTSP is the LSSS as defined by 10 CFR 50.36. However, use of the LTSP to define OPERABILITY in Technical Specifications would be an overly restrictive requirement if it were applied as an OPERABILITY limit for the "as-found" value of a protective device setting during a Surveillance.

BASES

BACKGROUND (continued)

However, there is also some point beyond which the device would have not been able to perform its function due, for example, to greater than expected drift. This value is specified in the SCP, as required by Specification 5.5.11, in order to define OPERABILITY of the devices and is designated as the Allowable Value which is the least conservative value of the as-found setpoint that a channel can have during CHANNEL CALIBRATION. The LTSP, $NTSP_F$, Allowable Value, "as-found" tolerance, and "as-left" tolerance, and the methodology for calculating the "as-left" and "as-found" tolerances will be maintained in the SCP, as required by Specification 5.5.11.

The Allowable Value is the least conservative value that the setpoint of the channel can have when tested such that a channel is OPERABLE if the setpoint is found conservative with respect to the Allowable Value during the CHANNEL CALIBRATION. Note that, although a channel is OPERABLE under these circumstances, the setpoint must be left adjusted to a value within the established "as-left" tolerance of the $NTSP_F$ and confirmed to be operating within the statistical allowances of the uncertainty terms assigned in the setpoint calculation. As such, the Allowable Value differs from the $NTSP_F$ by an amount equal to or greater than the "as-found" tolerance value. In this manner, the actual setting of the device will ensure that a SL is not exceeded or that automatic protective actions will initiate consistent with the design basis at any given point of time as long as the device has not drifted beyond that expected during the surveillance interval. If the actual setting of the device is found to be non-conservative with respect to the Allowable Value the device would be considered inoperable from a Technical Specification perspective. This requires corrective action including those actions required by 10 CFR 50.36 when automatic protective devices do not function as required.

The containment isolation function is performed by the Leak Detection and Isolation (LD&IS) portion of the Safety System Logic and Control/ Engineered Safety Features (SSLC/ESF) System. Functional diversity is provided by monitoring a wide range of independent parameters. Containment isolation occurs in response to signals from any of the following:

- Reactor Vessel Water Level - Low, Level 2,
- Reactor Vessel Water Level - Low, Level 1,
- Drywell Pressure - High,
- Main Steam Tunnel Ambient Temperature - High,
- RWCU/SDC Differential Mass Flow - High (per subsystem),

BASES

BACKGROUND (continued)

- Isolation Condenser Steam Line Flow - High (per Isolation Condenser),
- Isolation Condenser Condensate Return Line Flow - High (per Isolation Condenser),
- Isolation Condenser Pool Vent Discharge Radiation - High (per Isolation Condenser), or
- Reactor Building Exhaust Radiation – High.

The RWCU/SDC isolation function in MODES 5 and 6 is performed by the LD&IS portion of the SSLC/ESF System. RWCU/SDC isolation in MODES 5 and 6 isolation occurs in response to signals from either of the following:

- Reactor Vessel Water Level - Low, Level 2, or
- RWCU/SDC Differential Mass Flow - High (per subsystem),

The feedwater isolation function is performed by the LD&IS portion of the SSLC/ESF. Feedwater isolation occurs in response to any of the following:

- Feedwater Lines Differential Pressure - High concurrent with Drywell Pressure - High,
- Drywell Pressure - High concurrent with Drywell Water Level - High,
- Reactor Vessel Water Level - Low, Level 0.5, or
- Drywell Pressure - High-High.

The ICS isolation function that mitigates the accumulation of combustible gas is performed by the LD&IS portion of the SSLC/ESF. ICS isolation occurs in response to the following signal:

- Depressurization Valve – Open

At least 2 DPVs must be open for this ICS isolation to be initiated.

The HP CRD isolation function is performed by the LD&IS portion of the SSLC/ESF. HP CRD isolation occurs in response to any of the following:

- Drywell Pressure - High concurrent with Drywell Water Level - High, or
- Gravity-Driven Cooling System (GDCS) Pool Water Level - Low.

BASES

BACKGROUND (continued)

The SSLC/ESF controls the initiation signals and logic for isolation. SSLC/ESF is a four division, separated protection logic system designed to provide a very high degree of assurance to both ensure isolation when required and prevent inadvertent initiation. The input and output trip determinations for all isolation functions are based upon a two-out-of-four logic arrangement. Each division of SSLC/ESF is configured such that all functions (e.g., the digital trip module (DTM) function and voter logic unit (VLU) function) are implemented in triply redundant processors to support the requirement that single divisional failures cannot result in inadvertent actuation.

Four separate instrument channels are used to monitor isolation initiation parameters. Signals from sensors are multiplexed at the divisional level and triply redundant sensor data is then transmitted to the SSLC/ESF triply redundant DTM function for setpoint comparison. The output of each divisional DTM function (a trip/no-trip condition) is routed to all four divisional triply redundant VLU functions such that each divisional VLU function receives input from each of the four divisional DTM functions.

For maintenance purposes and added reliability, each DTM function has a division of sensors bypass such that all instruments in that division will be bypassed in the trip logic at the VLU functions. Thus, each VLU function will be making its trip decision on a two-out-of-three logic basis for each variable. It is possible for only one division of sensors bypass condition to be in effect at any time.

The processed trip signal from its own division and trip signals from the other three divisions are processed in the triply redundant VLU function for two-out-of-four voting.

The LD&IS logic is designed to seal-in the isolation signal once the trip has been initiated. The isolation signal overrides any control action to cause the closure of isolation valves. Reset of the isolation logic is required before any isolation valve can be manually opened.

Equipment within a single division is powered from the safety-related power source of the same division.

This Specification provides Operability requirements for the isolation instrumentation from the input variable sensors through the DTM function. Operability requirements for the isolation actuation circuitry consisting of timers, VLU functions, and load drivers are provided by LCO 3.3.6.4, "Isolation Actuation." Operability requirements for the actuated

BASES

BACKGROUND (continued)

components are addressed in LCO 3.6.1.3, "Containment Isolation Valves (CIVs)," and LCO 3.6.3.1, "Reactor Building (Contaminated Area Ventilation Subsystem (CONAVS) Area)."

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

The containment isolation signals generated by the isolation instrumentation are assumed in the safety analyses of References 1 and 2 to initiate closure of containment isolation valves and reactor building boundary isolation dampers to limit off-site doses. Refer to LCO 3.6.1.3, "Containment Isolation Valves (CIVs)," Applicable Safety Analyses Bases, for more detail on containment isolation valves and LCO 3.6.3.1, “Reactor Building (Contaminated Area Ventilation Subsystem (CONAVS) Area),” Applicable Safety Analyses Bases for more detail on reactor building boundary isolation dampers.

The RWCU/SDC isolation signals generated by the isolation instrumentation are assumed in the analyses of Reference 3 to initiate closure of the RWCU/SDC isolation valves to protect the core by minimizing a potential loss of reactor pressure vessel coolant inventory in MODES 5 and 6.

The feedwater isolation signals generated by the isolation instrumentation are assumed in the safety analyses of References 1 and 2 to initiate closure of feedwater isolation valves to limit mass water additions to the containment during and following a design basis feedwater line rupture inside containment.

The ICS isolation signals generated by the isolation instrumentation in response to the opening of 2 or more DPVs are assumed in the safety analyses of References 1 and 2 to mitigate the accumulation of radiolytic hydrogen and oxygen that could result in a detonation that would fail the ICS condensers and cause a breach of containment.

The HP CRD isolation signals generated by the isolation instrumentation are assumed in the safety analyses of References 1 and 2 to initiate closure of HP CRD makeup water injection isolation valves to limit mass water additions to the containment following a LOCA.

Isolation instrumentation satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii). However, certain monitored instrumentation parameters are retained for other reasons and are described below in the individual process parameter discussion.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

The OPERABILITY of the isolation instrumentation is dependent on the OPERABILITY of the individual instrumentation channel Functions specified in Table 3.3.6.3-1. Each Function must have the required number of OPERABLE channels, with their setpoints in accordance with the SCP, where appropriate. Each channel must also respond within its assumed response time, where appropriate. $NTSP_F$s are specified in the SCP, as required by Specification 5.5.11. The $NTSP_F$s are selected to ensure the setpoints are conservative with respect to the Allowable Value between successive CHANNEL CALIBRATIONS. Operation with a trip setpoint less conservative than the $NTSP_F$, but conservative with respect to its Allowable Value, is acceptable. A channel is inoperable if its actual trip setpoint is non-conservative with respect to its required Allowable Value.

In general, the individual monitored process parameters are required to be OPERABLE in MODES 1, 2, 3, and 4 consistent with the Applicability of LCO 3.6.1.3 and LCO 3.6.3.1. Functions that have different Applicabilities are discussed below in the individual Functions discussion.

Although there are four channels of isolation instrumentation for each function, only three channels of isolation instrumentation for each function are required to be OPERABLE. The three required channels are those channels associated with the DC and Uninterruptible AC Electrical Power Distribution Divisions required by LCO 3.8.6, "Distribution Systems - Operating." This is acceptable because the single-failure criterion is met with three OPERABLE isolation instrumentation channels, and because each isolation instrumentation division is associated with and receives power from only one of the four electrical divisions.

The specific Applicable Safety Analyses, LCO and specific Applicability discussions are provided below on a Function basis.

1. Reactor Vessel Water Level - Low, Level 2

Low reactor pressure vessel (RPV) water level indicates the capability to cool the fuel may be threatened. Should RPV water level decrease too far, fuel damage could result. The isolations of valves whose penetration communicate with the containment or the reactor vessel and the isolation of the reactor building boundary isolation dampers limit the release of fission products to help ensure that offsite does limits are not exceeded. The Reactor Vessel Water Level - Low, Level 2 is credited in the LOCA inside containment radiological analysis (Ref. 4).

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

In MODES 5 and 6, low RPV water level may indicate a loss of coolant. Should RPV water level decrease too far, the ability to cool the core may be threatened. Closure of the RWCU/SDC isolation valves isolates the system from the RPV, minimizing the potential loss of coolant inventory. The Reactor Vessel Water Level - Low, Level 2 is implicitly credited in the shutdown probabilistic risk assessment (Ref. 3), and therefore satisfies Criterion 4 of 10 CFR 50.36(c)(2)(ii).

Reactor Vessel Water Level - Low, Level 2 signals are initiated from four level sensors that sense the difference between the pressure due to a constant column (reference leg) of water and the pressure due to the actual water level (variable leg) in the vessel. Three channels of Reactor Vessel Water Level - Low, Level 2 Function are required to be OPERABLE to ensure no single instrument failure can preclude the isolation function.

The Reactor Vessel Water Level - Low, Level 2 Allowable Value was chosen to be the same as the Isolation Condenser System Reactor Vessel Water Level - Low, Level 2 Allowable Value.

This Function isolates the RWCU/SDC lines, Equipment and Floor Drain System lines, Containment Inerting System lines, and the Fuel and Auxiliary Pools Cooling System process lines.

<u>2. Reactor Vessel Water Level - Low, Level 1</u>

Low RPV water level indicates the capability to cool the fuel may be threatened. Should RPV water level decrease too far, fuel damage could result. The isolations of valves whose penetration communicate with the containment or the reactor vessel and the isolation of the reactor building boundary isolation dampers limit the release of fission products to help ensure that offsite does limits are not exceeded. The Reactor Vessel Water Level - Low, Level 1 channels are provided as a backup to the Reactor Vessel Water Level - Low, Level 2 channels and is not credited in the safety analysis.

Reactor Vessel Water Level - Low, Level 1 signals are initiated from four level sensors that sense the difference between the pressure due to a constant column (reference leg) of water and the pressure due to the actual water level (variable leg) in the vessel. Three channels of Reactor Vessel Water Level - Low, Level 1 Function are required to be OPERABLE to ensure no single instrument failure can preclude the isolation function.

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

The Reactor Vessel Water Level - Low, Level 1 Allowable Value was chosen to be the same as the Automatic Depressurization System Reactor Vessel Water Level - Low, Level 1 Allowable Value.

This Function isolates the RWCU/SDC lines, Process Radiation Monitoring System lines, Equipment and Floor Drain System lines, Containment Inerting System lines, Chilled Water System lines, and the Fuel and Auxiliary Pools Cooling System process lines.

3. Drywell Pressure - High

High drywell pressure can indicate a break in the reactor coolant pressure boundary. The isolations of valves whose penetration communicate with the containment and the isolation of the reactor building boundary isolation dampers limit the release of fission products to help ensure that offsite dose limits are not exceeded. The Drywell Pressure - High channels are not explicitly credited in the safety analyses but retained for the overall redundancy and diversity of the isolation instrumentation.

High drywell pressure signals are initiated from four pressure sensors that sense the pressure in the drywell. Three channels of Drywell Pressure - High are required to be OPERABLE to ensure no single instrument failure can preclude the isolation function.

The Drywell Pressure - High Allowable Value was chosen to be the same as the Reactor Protection System Drywell Pressure - High Allowable Value.

This Function isolates the Process Radiation Monitoring System lines, Equipment and Floor Drain System lines, Containment Inerting System lines, Chilled Water System lines, Fuel and Auxiliary Pools Cooling System process lines, and High Pressure Nitrogen Gas Supply System lines. In addition, this Function, in conjunction with either Feedwater Lines Differential Pressure - High or Drywell Water Level - High, isolates the feedwater lines. This Function, in conjunction with Drywell Water Level - High, also isolates the HP CRD makeup water injection line.

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

4. Main Steam Tunnel Ambient Temperature - High

Main Steam Tunnel Ambient Temperature - High Function is provided to detect a leak in the reactor coolant pressure boundary. The isolation occurs when a very small leak has occurred. If the small leak is allowed to continue without isolation, off-site dose limits may be reached. However, credit for these instruments is not taken in any transient or accident analysis because bounding analyses are performed for large breaks such as a MSL break.

Temperature signals are initiated from thermocouples located away from the main steam lines so they are only sensitive to ambient air temperature. Three channels of Main Steam Tunnel Temperature - High Function are required to be OPERABLE to ensure no single instrument failure can preclude the isolation function.

The ambient temperature monitoring Allowable Value is based on the room or compartment size and the cooling provisions of the ventilation system.

The Main Steam Tunnel Ambient Temperature - High Function isolates the RWCU/SDC System lines.

5. RWCU/SDC Differential Mass Flow - High (per subsystem)

The Reactor Water Cleanup/Shutdown Cooling (RWCU/SDC) System Differential Mass Flow - High signal is provided to detect a break in the RWCU System outside containment. Should the reactor coolant continue to flow out the break off-site dose limits may be exceeded. Therefore, isolation of the RWCU System is initiated when RWCU/SDC System Differential Mass Flow - High is sensed to prevent exceeding off-site doses. This Function is directly assumed in the RWCU/SDC System line failure event outside containment (Ref. 5).

In MODES 5 and 6, high RWCU/SDC differential flow may indicate a loss of coolant. Should RPV water level decrease too far, the ability to cool the core may be threatened. Closure of the RWCU/SDC isolation valves isolates the system from the RPV, minimizing the potential loss of coolant inventory. The Reactor Water Cleanup/Shutdown Cooling (RWCU/SDC) System Differential Mass Flow - High is implicitly credited in the shutdown probabilistic risk assessment (Ref. 3), and therefore satisfies Criterion 4 of 10 CFR 50.36(c)(2)(ii).

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

Each RWCU/SDC subsystem includes a suction line near the mid level of the reactor pressure level (RPV) and another suction line at the RPV bottom. Each suction line includes a venturi-type flow element inside containment. Each flow element is instrumented with four flow sensors. The temperature of each suction line is also monitored by four temperature elements close to the venturi-type flow element. Each RWCU/SDC subsystem also includes a return line to the feedwater lines and another return line to the overboarding lines. These lines are instrumented consistent with the suction lines. Each flow rate signal is converted to a mass flow rate signal using its associated temperature element. A differential flow rate is calculated from the difference between the suction flows and return flows. This differential flow rate is compared to the setpoint. Therefore, each differential flow channel consists of all the components necessary to calculate the differential flow signal and provide a trip signal.

Three channels of the RWCU/SDC System Differential Mass Flow - High Function per RWCU/SDC subsystem are required to be OPERABLE to ensure no single instrument failure can preclude the isolation function.

The RWCU/SDC System Differential Mass Flow - High Allowable Value ensures that a leak or a line break of the RWCU/SDC piping is detected.

This Function isolates the RWCU/SDC lines.

<u>6, 7, and 8. Isolation Condenser Steam and Condensate Return Line Flow - High and Pool Vent Discharge Radiation - High</u>

The Isolation Condenser Steam Line Flow - High, Condensate Return Line Flow - High, and Pool Vent Discharge Radiation - High Functions are provided to monitor the pressure boundary status of each individual Isolation Condenser System (ICS) subsystem. The Isolation Condenser Steam Line Flow - High and Condensate Return Line Flow - High Functions will isolate the associated subsystem when a leak or a break has occurred while the Pool Vent Discharge Radiation - High Function will isolate the associated subsystem when leakage is detected outside the drywell. These Functions are not assumed in any transient or accident analysis since bounding analyses are performed for large breaks such as MSL breaks.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

The isolation signals can be initiated from a total of 12 instruments per ICS subsystem, with each ICS subsystem having four differential pressure sensors per ICS subsystem steam line, four differential pressure sensors per ICS subsystem condensate line, and four radiation detectors located in its associated ICS subsystem vent discharge into the pool area. The flow instrumentation is designed to detect leakage both inside and outside of the drywell. The radiation detectors are designed to detect leakage outside of containment. Three channels of each monitored parameter for each ICS subsystem are required to be OPERABLE to ensure no single instrument failure can preclude the isolation functions.

The Allowable Value is chosen to be low enough to ensure that the isolation occurs to prevent fuel damage and maintains the MSL break event as the bounding event.

These Functions isolate the associated ICS lines.

9. Depressurization Valve – Open

The DPV – Open Function is provided to indicate that RPV depressurization has occurred and that the ICS is no longer required to perform its heat removal function. In this situation, the ICS is required to be isolated to mitigate the accumulation of radiolytic hydrogen and oxygen that could result in a detonation that would cause a containment breach. This Function is assumed in the safety analyses of References 1 and 2.

The position of each DPV is measured by 4 divisional position switches. The logic is arranged such that ICS Isolation will occur whenever 2 or more DPVs are open. Three channels of the DPV – Open Function are required to be OPERABLE for each DPV required by LCO 3.5.1, "Automatic Depressurization System (ADS) – Operating," to ensure no single instrument failure can preclude the isolation function.

This Function isolates the ICS lines.

10. Feedwater Lines Differential Pressure - High

The Feedwater Line Differential Pressure - High signal is provided to detect a break in the feedwater lines inside containment. Should the feedwater continue to flow into containment, containment integrity could be challenged as a result of the mass and energy addition to the containment drywell from the external feedwater system. Therefore,

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

isolation of the feedwater system flow is initiated when Feedwater Lines Differential Pressure - High is sensed to protect containment integrity. This Function is implicitly assumed in the safety analyses of References 1 and 2.

The differential pressure between the two feedwater lines is monitored by four divisions of LD&IS. A high differential pressure is indicative of a feedwater line break inside and outside the containment.

Three channels of the Feedwater Line Differential Pressure - High Function are required to be OPERABLE to ensure that no single instrument failure can preclude the isolation function.

The Feedwater Line Differential Pressure - High Allowable Value ensures that a leak or a line break of the feedwater piping is detected, in accordance with the containment analyses (Ref. 1).

This Function in conjunction with the Drywell Pressure - High Function isolates the feedwater lines.

<u>11. Reactor Building Exhaust Radiation - High</u>

High radiation in the reactor building exhaust or the refueling area exhaust is an indication of fission gases from a leak or an accident. The release may have originated from the containment due to a break in the reactor coolant pressure boundary or the refueling floor due to a fuel handling accident. When a Reactor Building Exhaust Radiation - High signal is detected, the Reactor Building Heating, Ventilation and Air Conditioning System is isolated. This Function is assumed to be available during high energy line break conditions and during a LOCA because the reactor building is credited for hold up and as a plate out barrier.

The Reactor Building Exhaust Radiation - High signal is initiated from radiation detectors that are located on the ventilation exhaust piping coming from the reactor building. Three channels of the Reactor Building Exhaust Radiation - High Function are required to be OPERABLE to ensure no single instrument failure can preclude the isolation functions.

The Reactor Building Exhaust Radiation - High Allowable Value is chosen to ensure the RB is isolated prior to radioactivity release exceeding the assumptions of the offsite does analyses.

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

12. Drywell Water Level - High

High drywell water level is an indication of a possible line break inside containment. This Function is provided to ensure that feedwater and HP CRD are isolated in the event of a LOCA, but remains capable of coolant injection for other accident scenarios.

Drywell water level is monitored by four channels of water level instrumentation. Three channels of the Drywell Water Level - High Function are required to be OPERABLE to ensure no single instrument failure can preclude the isolation function.

The Drywell Water Level - High Allowable Value is chosen to be low enough to ensure feedwater isolation occurs, limiting the flow of condensate into containment in accordance with the containment analyses (Ref. 1).

This Function in conjunction with the Drywell Pressure - High Function isolates the feedwater lines and the HP CRD makeup water injection line.

13. Reactor Vessel Water Level - Low, Level 0.5

Low RPV water level indicates the capability to cool the fuel may be threatened. Should RPV water level decrease too far, fuel damage could result. The isolations of valves whose penetration communicate with the containment or the reactor vessel limit the release of fission products to help ensure that offsite does limits are not exceeded. Reactor Vessel Water Level - Low, Level 0.5 signals are initiated from four fuel zone level sensors.

The Reactor Vessel Water Level - Low, Level 0.5 Allowable Value is chosen to ensure that feedwater line isolations occurs in accordance with the assumptions of Reference 4.

Three channels of Reactor Vessel Water Level - Low, Level 0.5 Function are required to be OPERABLE to ensure that no single instrument failure can preclude feedwater line isolation.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

14. Drywell Pressure - High-High

High drywell pressure is an indication of a possible line break inside containment. This Function is provided to ensure that feedwater is isolated in the event of a LOCA, but remains capable of coolant injection for other accident scenarios.

Drywell pressure is monitored by four channels of pressure instrumentation. Three channels of the Drywell Pressure - High-High Function are required to be OPERABLE to ensure no single instrument failure can preclude the isolation function.

The Drywell Pressure - High-High Allowable Value is chosen to be higher than the scram setpoint to prevent undesired initiation, and low enough to retain effectiveness throughout the entire spectrum of LOCA events.

This Function isolates the feedwater lines.

15. Gravity-Driven Cooling System Pool Water Level - Low

Low GDCS pool water level indicates the injection of water from the GDCS pools in the event of a LOCA. This Function is provided to ensure that the HP CRD makeup water injection is isolated to prevent the long-term addition of inventory to the containment following GDCS injection in response to a LOCA.

GDCS pool water level is monitored by four channels of water level indication in each GDCS pool. Three channels of the GDCS Pool Water Level - Low Function are required to be OPERABLE in each GDCS pool. This Function initiates upon a low level in two out of the three GDCS pools.

The GDCS Pool Water Level - Low Allowable Value is determined by analysis to ensure effectiveness under the full spectrum of LOCA events.

This Function isolates the HP CRD makeup water injection line.

ACTIONS

The ACTIONS are modified by two NOTES. Note 1 allows penetration flow path(s) to be unisolated intermittently under administrative controls. These controls consist of stationing a dedicated operator at the controls of the valve, who is in continuous communication with the control room. In this way, the penetration flow path can be rapidly isolated when a need

BASES

ACTIONS (continued)

for isolation is indicated. Note 2 has been provided to modify the ACTIONS related to Isolation Instrumentation channels. Section 1.3, Completion Times, specifies once a Condition has been entered, subsequent divisions, subsystems, components or variables expressed in the Condition discovered to be inoperable or not within limits, will not result in separate entry into the Condition. Section 1.3 also specifies Required Actions of the Condition continue to apply for each additional failure, with Completion Times based on initial entry into the Condition. However, the Required Actions for inoperable Isolation Instrumentation channels provide appropriate compensatory measures for separate inoperable channels. As such, a Note has been provided which allows separate Condition entry for each inoperable Isolation Instrumentation channel.

A.1

With one or more Functions with one required channel inoperable, the affected required channel must be restored to OPERABLE status within 12 hours. The 12-hour Completion Time is acceptable based on engineering judgment considering the diversity of sensors available to provide isolation signals, the redundancy of the isolation design, and the low probability of an event requiring isolation during this interval. However, this out of service time is only acceptable provided the associated Function still maintains isolation capability (refer to Required Actions B.1 Bases). If the inoperable required channel cannot be restored to OPERABLE status within the 12-hour Completion Time, the affected instrumentation division must be verified to be in trip. This is acceptable because verifying the affected isolation instrumentation division in trip conservatively compensates for the inoperability by placing the isolation instrumentation in a one-out-of-two configuration, restoring the capability to accommodate a single failure.

Alternatively, if it is not desirable to verify the required instrument channel in trip (as in the case where it is desirable to place the affected channel of sensors in bypass), Condition C must be entered and its Required Action taken when the Completion Time of Required Action A.1 expires.

B.1

This Required Action directs entry into the appropriate Condition referenced in Table 3.3.6.3-1 if the Required Action and Completion Time of Condition A is not met or if multiple, inoperable, untripped required channels for the same Function result in the Function not maintaining

ACTIONS (continued)

isolation capability. A Function is considered to be maintaining isolation capability when sufficient channels are OPERABLE or in trip such that the isolation logic will generate a trip signal from the given Function on a valid signal so that at least one valve in the associated penetration flow path is isolated. The applicable Condition specified in the Table is Function and MODE or other specified condition dependent and may change as the Required Action of a previous Condition is completed.

C.1

If the affected instrumentation channel cannot be verified to be in trip within the specified Completion Time or if isolation capability is not maintained, plant operations may continue if the associated Containment Isolation Valve(s) (CIVs) is declared inoperable immediately. Because this Function is required to ensure that the CIVs perform their intended function, sufficient remedial measures are provided by declaring the associated CIV(s) inoperable.

D.1 and D.2

If the affected instrumentation channel cannot be verified to be in trip within the specified Completion Time or if isolation capability is not maintained, 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 12 hours and to MODE 5 within 36 hours. The Completion Time is reasonable, based on plant design, to reach required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

E.1 and E.2

If the affected instrumentation channel cannot be verified to be in trip within the specified Completion Time or if isolation capability is not maintained, the associated flow path should be isolated. However, if the RWCU/SDC function is needed to provide core cooling, these Required Actions allow the flow path to remain unisolated provided action is immediately initiated to restore the channel to OPERABLE status or to isolate the RWCU/SDC system (i.e., provide alternate decay heat removal capabilities so the flow path can be isolated). ACTIONS must continue until the channel is restored to OPERABLE status or the RWCU/SDC system is isolated.

BASES

SURVEILLANCE REQUIREMENTS

As noted at the beginning of the Surveillance Requirements, the SRs for each isolation instrumentation Function are located in the SRs column of Table 3.3.6.3-1.

SR 3.3.6.3.1

Performance of the CHANNEL CHECK once every 12 hours ensures that a gross failure of instrumentation has not occurred.

The SSLC/ESF is cyclically tested from the sensor input point to the logic contact output by online self-diagnostics. The self-diagnostic capabilities include microprocessor checks, system initialization, watchdog timers, memory integrity checks, input/output (I/O) data integrity checks, communication bus interface checks, and checks on the application program (checksum).

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 unit staff, based on a combination of the channel instrument uncertainties, including indication, and readability. If a channel is outside the match criteria, it may be an indication that the instrument has drifted outside its limit.

The Surveillance Frequency is based on operating experience that demonstrates channel failure is rare.

The CHANNEL CHECK supplements less formal, but more frequent checks of channels during normal operational use of the displays associated with the LCO required channels.

SR 3.3.6.3.2

A CHANNEL FUNCTIONAL TEST is performed on each required channel to ensure that the channel will perform the intended function. This test ensures a complete CHANNEL FUNCTIONAL TEST of required instrument channels from the sensor input through the DTM function.

The SSLC/ESF is cyclically tested from the sensor input point to the logic contact output by online self-diagnostics. The self-diagnostic capabilities include microprocessor checks, system initialization, watchdog timers, memory integrity checks, input/output (I/O) data integrity checks, communication bus interface checks, and checks on the application program (checksum).

BASES

SURVEILLANCE REQUIREMENTS (continued)

The Frequency of 31 days is based on the reliability of the Isolation Instrumentation channels and the self-diagnostic features that monitor the channels for proper operation.

SR 3.3.6.3.3

CHANNEL CALIBRATION is a complete check of the instrument loop and the sensor. This test verifies that the required channel responds to the measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the required channel adjusted to the $NTSP_F$ within the "as-left" tolerance to account for instrument drifts between successive calibrations consistent with the methods and assumptions required by the SCP.

The Surveillance Frequency is based on the assumption of a 24 month calibration interval in the determination of the magnitude of equipment drift in the setpoint analysis.

SR 3.3.6.3.4

This SR ensures that the individual required channel response times are less than or equal to the maximum values assumed in the accident analysis. The instrument response times must be added to the associated closure times to obtain the ISOLATION SYSTEM RESPONSE TIME. ISOLATION SYSTEM RESPONSE TIME acceptance criteria are included in Reference 6.

ISOLATION SYSTEM RESPONSE TIME may be verified by actual response time measurements in any series of sequential, overlapping, or total channel measurements. This test encompasses the isolation instrumentation from the input variable sensors through the DTM function. This test overlaps the testing required by SR 3.3.6.4.2 to ensure complete testing of instrumentation channels and actuation circuitry.

A Note to the Surveillance states that the radiation detectors may be excluded from ISOLATION SYSTEM RESPONSE TIME testing. This Note is necessary because of the difficulty of generating an appropriate detector input signal and because the principles of detector operation virtually ensure an instantaneous response time. Response Time for radiation detection channels shall be measured from detector output or the input of the first electronic component in the channel.

BASES

SURVEILLANCE REQUIREMENTS (continued)

COL 16.0-1-A
3.3.6.3-2

[However, some sensors are allowed to be excluded from specific ISOLATION SYSTEM RESPONSE TIME measurement if the conditions of Reference XX are satisfied. If these conditions are satisfied, sensor response time may be allocated based on either assumed design sensor response time or the manufacturer's stated design response time. When the requirements of Reference XX are not satisfied, sensor response time must be measured. Furthermore, measurement of the instrument loops response time for some Functions is not required if the conditions of Reference XX are satisfied.]

ISOLATION SYSTEM RESPONSE TIME tests are conducted on a 24-month STAGGERED TEST BASIS for three channels. The Frequency of 24 months on a STAGGERED TEST BASIS ensures that the required channels associated with each division are alternately tested. The 24-month test Frequency is consistent with the refueling cycle and has with operating experience that shows that random failures of instrumentation components causing serious response time degradation, but not channel failure, are infrequent.

REFERENCES

1. Section 6.2.

2. Chapter 15.

3. NEDO-33201, ESBWR Certification Probabilistic Risk Assessment, Revision 6, October 2010.

4. Subsection 15.4.4.

5. Subsection 15.4.9.

6. Section 15.2.

B 3.3 INSTRUMENTATION

B 3.3.6.4 Isolation Actuation

BASES

BACKGROUND

The isolation actuation logic is designed to isolate the affect penetration flow paths when one or more monitored parameters exceed the specified limit. The isolation actuation logic actuates the following containment isolation flow paths: (a) Reactor Water Cleanup/Shutdown Cooling (RWCU/SDC) System lines, (b) Isolation Condenser System (ICS) lines, (c) Process Radiation Monitoring System lines, (d) Equipment and Floor Drain System lines, (e) Containment Inerting System lines, (f) Chilled Water System lines, (g) Fuel and Auxiliary Pools Cooling System (FAPCS) process lines, and (h) High Pressure Nitrogen Gas Supply System lines. The isolation actuation logic also isolates the reactor building boundary isolation dampers. The function of the containment isolation valves and reactor building boundary isolation dampers, in combination with other accident mitigation systems, is to limit fission product release during postulated Design Basis Accidents (DBAs). Containment and reactor building isolation within the times specified ensure that the release of radioactive materials to the environment will be consistent with the assumptions used in the analysis of DBAs.

The isolation actuation logic is also designed to isolate the RWCU/SDC System from the reactor pressure vessel (RPV) in MODES 5 and 6, isolate feedwater flow into containment and trip main feedwater pump breakers, isolate the ICS when 2 or more Depressurization Valves (DPVs) are open, and isolate high pressure control rod drive (HP CRD) makeup water injection when one or more monitored parameters exceed the specified limit. The function of the feedwater isolation valves is to limit the mass addition of water into containment during and following a design basis feedwater line rupture inside containment. The function of the reactor water cleanup/shutdown cooling (RWCU/SDC) isolation valves in MODES 5 and 6 is to protect the core by isolating the RWCU/SDC system from the reactor pressure vessel and minimizing a potential loss of coolant resulting from a line break in the RWCU/SDC system. The function of the ICS isolation that occurs when 2 or more DPVs are open is to mitigate the accumulation of radiolytic hydrogen and oxygen that could result in a detonation. The function of the HP CRD makeup water isolation is to prevent the long-term addition of inventory to the containment following a loss of coolant accident (LOCA).

A detailed description of the isolation instrumentation and isolation actuation logic is provided in the Bases for LCO 3.3.6.3, "Isolation Instrumentation."

BASES

BACKGROUND (continued)

This Specification provides Operability requirements for the isolation actuation circuitry consisting of timers, voter logic unit (VLU) functions, and load drivers. Operability requirements for the isolation instrumentation from the input variable sensors through the DTM function are provided by LCO 3.3.6.3, "Isolation Instrumentation." Operability requirements for the actuated components are addressed in LCO 3.6.1.3, "Containment Isolation Valves (CIVs)," and LCO 3.6.3.1, "Reactor Building (Contaminated Area Ventilation Subsystem (CONAVS) Area)."

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

The containment isolation signals generated by the isolation instrumentation are assumed in the safety analyses of References 1 and 2 to initiate closure of valves and reactor building boundary isolation dampers to limit off site doses. Refer to LCO 3.6.1.3, Applicable Safety Analyses, for more details of containment isolation valves. Refer to LCO 3.6.3.1, Applicable Safety Analyses, for more details of the reactor building isolation dampers.

The RWCU/SDC isolation signals generated by the isolation instrumentation are assumed in the analyses of Reference 3 to initiate closure of the RWCU/SDC isolation valves to protect the core by minimizing a potential loss of reactor pressure vessel coolant inventory in MODES 5 and 6.

The feedwater isolation signals generated by the isolation instrumentation are assumed in the safety analyses of References 1 and 2 to initiate closure of feedwater isolation valves to limit mass water additions to the containment during and following a design basis feedwater line rupture inside containment.

The ICS isolation signals generated by the isolation instrumentation in response to the opening of 2 or more DPVs are assumed in the safety analyses of References 1 and 2 to mitigate the accumulation of radiolytic hydrogen and oxygen that could result in a detonation that would fail the ICS condensers and cause a breach of containment.

The HP CRD isolation signals generated by the isolation instrumentation are assumed in the safety analyses of References 1 and 2 to initiate isolation of the HP CRD makeup water injection line to prevent the long-term addition of inventory to the containment following a LOCA.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

Isolation Actuation satisfies Criteria 3 and 4 of 10 CFR 50.36(c)(2)(ii).

Although there are four isolation actuation divisions, only three are required to be OPERABLE to ensure no single automatic actuation division failure will preclude an isolation to occur on a valid signal. The three required divisions are those divisions associated with the DC and Uninterruptible AC Electrical Power Distribution Divisions required by LCO 3.8.6, "Distribution Systems - Operating." This is acceptable because the single-failure criterion is still met with three OPERABLE isolation actuation divisions, and because each isolation division is associated with and receives power from only one of the four electrical divisions.

The individual containment isolation actuation divisions are required to be OPERABLE in the MODES 1, 2, 3, and 4 consistent with the Applicability of LCO 3.6.1.3 and LCO 3.6.3.1. The feedwater isolation valve actuation divisions are required to be OPERABLE in MODES 1, 2, 3, and 4 consistent with the assumptions of References 1 and 2. The RWCU/SDC isolation actuation division is also required to be OPERABLE in MODES 5 and 6 consistent with the assumptions of Reference 3.

1. Reactor Water Cleanup/Shutdown Cooling System Isolation

The RWCU/SDC System Isolation actuation divisions receive input from the following isolation instrumentation: Reactor Vessel Water Level - Low, Level 2; Reactor Vessel Water Level - Low, Level 1; Main Steam Tunnel Ambient Temperature - High; and Reactor Water Cleanup/Shutdown Cooling System Differential Mass Flow - High (per RWCU/SDC subsystem) Functions. In MODES 5 and 6, the RWCU/SDC System Isolation actuation divisions receive input from the Reactor Vessel Water Level - Low, Level 2 and from the Reactor Water Cleanup/Shutdown Cooling System Differential Mass Flow - High (Per RWCU/SDC subsystem) Functions. Three Reactor Water Cleanup/Shutdown Cooling System Isolation actuation divisions are required to be OPERABLE to ensure no single isolation actuation failure can preclude the isolation function.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

2. Isolation Condenser System Isolation

The Isolation Condenser System Isolation actuation divisions receive input from the following isolation instrumentation: Isolation Condenser Steam Line Flow - High (per ICS subsystem); Isolation Condenser Condensate Line Flow - High (per ICS subsystem); Isolation Condenser Pool Vent Discharge Radiation - High (per ICS subsystem); and Depressurization Valve - Open Functions. Three Isolation Condenser System Isolation actuation divisions are required to be OPERABLE to ensure no single isolation actuation failure can preclude the isolation function.

3. Process Radiation Monitoring System Isolation

The Process Radiation Monitoring System Isolation actuation divisions receive input from the following isolation instrumentation: Reactor Vessel Water Level - Low, Level 1; and Drywell Pressure - High Functions. Three Process Radiation Monitoring System Isolation actuation divisions are required to be OPERABLE to ensure no single isolation actuation failure can preclude the isolation function.

4. Equipment and Floor Drain System Isolation

The Equipment and Floor Drain System Isolation actuation divisions receive input from the following isolation instrumentation: Reactor Vessel Water Level - Low, Level 2; Reactor Vessel Water Level - Low, Level 1; and Drywell Pressure High Functions. Three Equipment and Floor Drain System Isolation actuation divisions are required to be OPERABLE to ensure no single isolation actuation failure can preclude the isolation function.

5. Containment Inerting System Isolation

The Containment Inerting System Isolation actuation divisions receive input from the following isolation instrumentation: Reactor Vessel Water Level - Low, Level 2; Reactor Vessel Water Level - Low, Level 1 and Drywell Pressure - High Functions. Three Containment Inerting System Isolation actuation divisions are required to be OPERABLE to ensure no single isolation actuation failure can preclude the isolation function.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

6. Chilled Water System Isolation

The Chilled Water System Isolation actuation divisions receive input from the following isolation instrumentation: Reactor Vessel Water Level - Low, Level 1; and Drywell Pressure - High Functions. Three Chilled Water System Isolation actuation divisions are required to be OPERABLE to ensure no single isolation actuation failure can preclude the isolation function.

7. Fuel and Auxiliary Pools Cooling System Process Lines

The FAPCS Process Lines isolation actuation divisions receive input from the following isolation instrumentation: the Reactor Vessel Water Level - Low, Level 2; Reactor Vessel Water Level - Low, Level 1; and Drywell Pressure - High Functions. Three FAPCS Process Lines isolation actuation divisions are required to be OPERABLE to ensure no single isolation actuation failure can preclude the isolation function.

8. Reactor Building Heating, Ventilation and Air Conditioning System Isolation

Reactor Building Heating, Ventilation and Air Conditioning System Isolation actuation divisions receive input from the Reactor Building Exhaust Radiation - High. Three Reactor Building Heating, Ventilation and Air Conditioning System Isolation actuation divisions are required to be OPERABLE to ensure no single isolation actuation failure can preclude the isolation function.

9. High Pressure Nitrogen Gas Supply Isolation

The High Pressure Nitrogen Gas Supply Isolation actuation divisions receive input from the following isolation instrumentation: Reactor Vessel Water Level - Low, Level 1; and Drywell Pressure - High Functions. Three High Pressure Nitrogen Gas Supply isolation actuation divisions are required to be OPERABLE to ensure no single isolation actuation failure can preclude the isolation function.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

10. Feedwater Isolation Valves Isolation

The Feedwater Isolation Valve Isolation actuation divisions receive input from the Feedwater Lines Differential Pressure - High, Drywell Water Level - High, Reactor Vessel Level - Low, Level 0.5, Drywell Pressure - High, and Drywell Pressure - High-High isolation instrumentation channels. Each feedwater line includes one feedwater control valve installed as the inboard containment isolation valve and the first of two in-series feedwater isolation valves is installed as the outboard containment isolation valve. The second feedwater isolation valve and feedwater control valve provide functional redundancy. This Function actuates the two feedwater isolation valves in each feedwater line to provide isolation in the event of a feedwater line break inside containment. Three Feedwater Isolation Valve - Isolation actuation divisions are required to be OPERABLE to ensure that no single isolation actuation failure can preclude the Function.

11. High Pressure Control Rod Drive Isolation

The HP CRD Isolation actuation divisions receive input from the Gravity Driven-Driven Cooling System (GDCS) Pool Water Level - Low, Drywell Pressure - High, and Drywell Water Level - High isolation instrumentation channels. The HP CRD makeup water injection line contains two in-series isolation valves. This Function actuates the two isolation valves in the HP CRD makeup water injection line to prevent addition of inventory to the containment by this pathway following a LOCA. Three HP CRD Isolation actuation divisions are required to be OPERABLE to ensure that no single isolation actuation failure can preclude the isolation function.

ACTIONS

The ACTIONS are modified by two NOTES. Note 1 allows penetration flow path(s) to be unisolated intermittently under administrative controls. These controls consist of stationing a dedicated operator at the controls of the valve, who is in continuous communication with the control room. In this way, the penetration flowpath can be rapidly isolated when a need for isolation is indicated. Note 2 has been provided to modify the ACTIONS related to isolation actuation. Section 1.3, Completion Times, specifies once a Condition has been entered, subsequent divisions, subsystems, components or variables expressed in the Condition discovered to be inoperable or not within limits, will not result in separate entry into the Condition. Section 1.3 also specifies Required Actions of the Condition continue to apply for each additional failure, with

BASES

ACTIONS (continued)

Completion Times based on initial entry into the Condition. However, the Required Actions for inoperable isolation actuation provides appropriate compensatory measures for separate inoperable isolation actuation divisions. As such, a Note has been provided which allows separate Condition entry for each inoperable isolation actuation division.

A.1

The 4-hour Completion Time is consistent with the Completion Times of LCO 3.6.1.3 for penetration flow paths with two CIVs and is acceptable based on engineering judgment considering the diversity of sensors available to provide isolation signals, the redundancy of the isolation design, and the low probability of an accident requiring isolation during this time. However, this out of service time is only acceptable provided the associated Function still maintains isolation actuation capability (refer to Required Actions B.1 Bases). If the inoperable division cannot be restored to OPERABLE status within the 4-hour Completion Time, the affected required actuation division must be verified to be in trip. This is acceptable because verifying the affected isolation actuation division in trip conservatively compensates for the inoperability by placing the isolation actuation in a one-out-of-two configuration, restoring the capability to accommodate a single failure.

Alternatively, if it is not desirable to verify the affected required actuation division in trip (as in the case where it is desired to place the affected division in bypass), Condition C must be entered and its Required Action taken when the Completion Time of Required Action A.1 expires.

B.1

This Required Action directs entry into the appropriate Condition referenced in Table 3.3.6.4-1 if the Required Action and Completion Time of Condition A is not met or if multiple, inoperable, untripped required divisions of isolation actuation (i.e., one or two divisions associated with each isolation valve or damper in a penetration flow path) result in the isolation actuation capability not maintained. Isolation automatic actuation capability is considered to be maintained when sufficient actuation divisions are OPERABLE or in trip such that the isolation logic will generate a trip signal on a valid signal to close one valve on the associated penetration. The applicable Condition specified in the Table is Function and MODE or other specified condition dependent and may change as the Required Action of a previous Condition is completed.

BASES

ACTIONS (continued)

C.1

With the Required Action and associated Completion Time of Condition A not met, or if isolation actuation capability is not maintained, the affected isolation actuation device(s) must be declared inoperable immediately. Isolation actuation capability is considered to be maintained when sufficient actuation divisions are OPERABLE such that isolation logic will generate an actuation signal on a valid signal.

D.1 and D.2

With the Required Action and associated Completion Time of Condition A not met, or if two or more required actuation divisions inoperable, 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 12 hours and to MODE 5 within 36 hours The Completion Time is reasonable, based on plant design, to reach required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

E.1 and E.2

If the affected actuation division cannot be verified to be in trip within the specified Completion Time or if isolation capability is not maintained, the associated flow path should be isolated. However, if the RWCU/SDC function is needed to provide core cooling, these Required Actions allow the flow path to remain unisolated provided action is immediately initiated to restore the division to OPERABLE status or to isolate the RWCU/SDC system (i.e., provide alternate decay heat removal capabilities so the flow path can be isolated). ACTIONS must continue until the division is restored to OPERABLE status or the RWCU/SDC system is isolated.

SURVEILLANCE REQUIREMENTS

As noted at the beginning of the SRs, the SRs for each isolation actuation Function are located in the SRs column of Table 3.3.6.4-1.

SR 3.3.6.4.1

The LOGIC SYSTEM FUNCTIONAL TEST demonstrates the OPERABILITY of the isolation actuation divisions. The testing in LCO 3.3.6.3, LCO 3.6.1.3, and LCO 3.6.3.1 overlaps this Surveillance to provide complete testing of the assumed safety function.

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 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 24-month Frequency.

SR 3.3.6.4.2

This SR ensures that the individual required division response times are less than or equal to the maximum values assumed in the accident analysis. The instrument response times must be added to the associated closure times to obtain the ISOLATION SYSTEM RESPONSE TIME. ISOLATION SYSTEM RESPONSE TIME acceptance criteria are included in Reference 4.

ISOLATION SYSTEM RESPONSE TIME may be verified by actual response time measurements in any series of sequential, overlapping, or total channel measurements. This test encompasses the isolation actuation circuitry consisting of timers, VLU functions, and load drivers. This test overlaps the testing required by SR 3.3.6.3.4 to ensure complete testing of instrumentation channels and actuation divisions.

COL 16.0-1-A 3.3.6.4-1

[However, some portions of the isolation actuation circuitry are allowed to be excluded from specific ISOLATION SYSTEM RESPONSE TIME measurement if the conditions of Reference XX are satisfied. Furthermore, measurement of the instrument loops response time for some Functions is not required if the conditions of Reference XX are satisfied.]

ISOLATION SYSTEM RESPONSE TIME tests are conducted on a 24-month STAGGERED TEST BASIS for three divisions. The Frequency of 24 months on a STAGGERED TEST BASIS ensures that the channels associated with each required division are alternately tested. The 24-month test Frequency is consistent with the refueling cycle and with operating experience that shows that random failures of instrumentation components causing serious response time degradation, but not channel failure, are infrequent.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.6.4.3

A system functional test is performed to verify that the mechanical portions of the actuation function operate as designed when demanded. This includes verifying that RWCU/SDC isolation valves, feedwater isolation valves, and HP CRD makeup water injection isolation valves automatically close. The LOGIC SYSTEM FUNCTIONAL TEST in SR 3.3.6.4.1 and LCO 3.3.8.1 (for RWCU/SDC isolation valves) overlaps this SR to provide complete testing of the safety function.

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 an unplanned transient if the Surveillance were performed with the reactor at power.

REFERENCES

1. Section 6.2.
2. Chapter 15.
3. NEDO-33201, ESBWR Certification Probabilistic Risk Assessment, Revision 6, October 2010.
4. Section 15.2.

B 3.3 INSTRUMENTATION

B 3.3.7.1 Control Room Habitability Area (CRHA) Heating, Ventilation, and Air Conditioning (HVAC) Subsystem (CRHAVS) Instrumentation

BASES

BACKGROUND

COL 16.0-1-A 3.3.7.1-2

The purpose of the CRHAVS instrumentation is to initiate appropriate actions to ensure the CRHAVS and control room habitability area (CRHA) boundary provide a protected environment from which occupants can control the unit following an uncontrolled release of radioactivity[or hazardous chemicals]. The equipment involved with CRHAVS is described in the Bases for LCO 3.7.2, "Control Room Habitability Area (CRHA) Heating, Ventilation, and Air Conditioning (HVAC) Subsystem (CRHAVS)."

The safety-related function of the CRHAVS used to control radiation exposure consists of two independent and redundant high efficiency air filtration subsystems, or Emergency Filter Units (EFUs), for treatment of outside supply air and a CRHA boundary that limits the inleakage of unfiltered air. Upon receipt of a high control room air intake radiation initiation signal (indicative of conditions that could result in radiation exposure to CRHA occupants), or upon an extended loss of AC power, the CRHA isolation mode is initiated as follows:

- The primary divisional fan of the primary EFU is energized,
- The primary EFU redundant isolation dampers are opened,
- The main air supply duct and restroom exhaust isolation dampers are closed, and
- The nonsafety-related normal ventilation fans are stopped.

If all onsite and offsite AC power is lost, one of the nonsafety-related recirculation AHUs operates for a minimum of two hours using the nonsafety-related Uninterruptible AC Power Supply System to dissipate heat from operation of the nonsafety-related main control room Nonsafety-Related Distributed Control and Information System (N-DCIS) electrical loads. Selected N-DCIS electrical loads are automatically de-energized upon receipt of a CRHA high temperature initiation signal (indicating failure of the redundant nonsafety-related recirculation AHUs).

BASES

BACKGROUND (continued)

During operation of the EFU, the standby selected EFU is automatically started upon receipt of a EFU outlet high radiation or EFU low flow initiation signal (indicating failure of the selected primary EFU filters or fans to operate). Controls to manually isolate the CRHA and to manually actuate CRHAVS following indication of a radiological event (indicative of conditions that could result in radiation exposure to CRHA occupants) are provided.

CRHAVS operation in maintaining CRHA habitability is discussed in Section 6.4 and Section 9.4.1 (Refs. 1 and 2, respectively).

Technical Specifications are required by 10 CFR 50.36 to contain Limiting Safety System Settings (LSSS) defined by the regulation as "...settings for automatic protective devices related to those variables having significant safety functions." Where LSSS is specified for a variable on which a Safety Limit (SL) has been placed, the setting must be chosen such that automatic protective action will correct the abnormal situation before a SL is exceeded. The Analytical Limit is the limit of the process variable at which a safety action is initiated, as established by the safety analysis, to ensure that a SL is not exceeded. Any automatic protection action that occurs on reaching the Analytical Limit therefore ensures that the SL is not exceeded. Where LSSS is specified for a variable having a significant safety function but which does not protect SLs, the setting must be chosen such that automatic protective actions will initiate consistent with the design basis. The Design Limit is the limit of the process variable at which a safety action is initiated to ensure that these automatic protective devices will perform their specified safety function.

The actual settings for automatic protective devices must be chosen to be more conservative than the Analytical / Design Limit to account for instrument loop uncertainties related to the setting at which the automatic protective action would actually occur. The methodology for determining the actual settings, and the required tolerances to maintain these settings conservative to the Analytical / Design Limits, including the requirements for determining that the channel is OPERABLE, are defined in the Setpoint Control Program (SCP), in accordance with Specification 5.5.11, "Setpoint Control Program (SCP)."

BASES

BACKGROUND (continued)

The Limiting Trip Setpoint (LTSP) is a predetermined setting for a protective device chosen to ensure automatic actuation prior to the process variable reaching the Analytical / Design Limit and thus ensuring that the SL would not be exceeded (i.e., for Analytical Limits), or that automatic protective actions occur consistent with the design basis (i.e., for Design Limits). As such, the LTSP accounts for process and primary element measurement errors, and uncertainties in setting the device (e.g., calibration), uncertainties in how the device might actually perform (e.g., accuracy), changes in the point of action of the device over time (e.g., drift during surveillance intervals), and any other factors that may influence its actual performance (e.g., harsh accident environments). In this manner, the LTSP ensures that SLs are not exceeded and that automatic protective devices will perform their specified safety function. As such, the LTSP meets the definition of an LSSS. The nominal trip setpoint to which the setpoint is reset after calibration is the $NTSP_F$, which is more conservative than the LTSP and has margin to assure that the Allowable Value is not exceeded during calibration.

Technical Specifications contain values related to the OPERABILITY of equipment required for safe operation of the facility. OPERABLE is defined in Technical Specifications as "...being capable of performing its safety function(s)." For automatic protective devices, the required safety function is to ensure that a SL is not exceeded and that automatic protective actions will initiate consistent with the design basis. Therefore, the LTSP is the LSSS as defined by 10 CFR 50.36. However, use of the LTSP to define OPERABILITY in Technical Specifications would be an overly restrictive requirement if it were applied as an OPERABILITY limit for the "as-found" value of a protective device setting during a Surveillance.

However, there is also some point beyond which the device would have not been able to perform its function due, for example, to greater than expected drift. This value is specified in the SCP, as required by Specification 5.5.11, in order to define OPERABILITY of the devices and is designated as the Allowable Value, which is the least conservative value of the as-found setpoint that a channel can have during CHANNEL CALIBRATION. The LTSP, $NTSP_F$, Allowable Value, "as-found" tolerance, and "as-left" tolerance, and the methodology for calculating the "as-left" and "as-found" tolerances will be maintained in the SCP, as required by Specification 5.5.11.

BACKGROUND (continued)

The Allowable Value is the least conservative value that the setpoint of the channel can have when tested such that a channel is OPERABLE if the setpoint is found conservative with respect to the Allowable Value during the CHANNEL CALIBRATION. Note that, although a channel is OPERABLE under these circumstances, the setpoint must be left adjusted to a value within the established "as-left" tolerance of the $NTSP_F$ and confirmed to be operating within the statistical allowances of the uncertainty terms assigned in the setpoint calculation. As such, the Allowable Value differs from the $NTSP_F$ by an amount equal to or greater than the "as-found" tolerance value. In this manner, the actual setting of the device will ensure that a SL is not exceeded or that automatic protective actions will initiate consistent with the design basis at any given point of time as long as the device has not drifted beyond that expected during the surveillance interval. If the actual setting of the device is found to be non-conservative with respect to the Allowable Value the device would be considered inoperable from a Technical Specification perspective. This requires corrective action including those actions required by 10 CFR 50.36 when automatic protective devices do not function as required.

The Safety System Logic and Control/Engineered Safety Features (SSLC/ESF) System controls the initiation signals and logic for CRHA isolation, CRHAVS actuation, and N-DCIS electrical load de-energization. SSLC/ESF is a four division, separated protection logic system designed to provide a very high degree of assurance to both ensure CRHA isolation, CRHAVS actuation, and N-DCIS electrical load de-energization when required, and prevent inadvertent isolation, actuation, and de-energization. The input and output trip determinations for all CRHAVS functions are based upon a two-out-of-four logic arrangement. Each division of SSLC/ESF is configured such that all functions (e.g., the digital trip module (DTM) function and voter logic unit (VLU) function) are implemented in triply redundant processors to support the requirement that single divisional failures cannot result in inadvertent actuation.

Four separate instrument channels are used to monitor CRHAVS initiation parameters. Signals from sensors are multiplexed at the divisional level and triply redundant sensor data is then transmitted to the PRMS and SSLC/ESF triply redundant DTM function for setpoint comparison. The output of each divisional DTM (a trip/no-trip condition) is routed to all four divisional triply redundant VLU functions such that each divisional VLU function receives input from each of the four divisional DTM functions.

BASES

BACKGROUND (continued)

For maintenance purposes and added reliability, each DTM function has a division of sensors bypass such that all instruments in that division will be bypassed in the trip logic at the VLU functions. Thus, each VLU function will be making its trip decision on a two-out-of-three logic basis for each variable. It is possible for only one division of sensors bypass condition to be in effect at any time.

The processed trip signal from its own division and trip signals from the other three divisions are processed in the triply redundant VLU function for two-out-of-four voting.

The load driver arrangement for actuation of the CRHA isolation dampers, CRHAVS fans and dampers, and N-DCIS electrical load breakers are such that an actuation signal from two divisions of CRHA isolation, CRHAVS actuation, and N-DCIS electrical load de-energization logic are required to actuate each damper, fan, or breaker.

Although an actuation signal from any two divisions provides the start signal for all four EFU fans with their associated dampers, the SSLC/ESF logic allows only one designated EFU fan to start in the designated primary EFU.

This Specification provides OPERABILITY requirements for the CRHA isolation, CRHAVS actuation, and N-DCIS electrical load de-energization instrumentation from the input variable sensors through the DTM function. OPERABILITY requirements for the CRHA isolation, CRHAVS actuation, and N-DCIS electrical load de-energization instrumentation circuitry consisting of VLU functions and load drivers are provided by LCO 3.3.7.2, "Control Room Habitability Area (CRHA) Heating, Ventilation, and Air Conditioning (HVAC) Subsystem (CRHAVS) Actuation." OPERABILITY requirements for the actuated components are addressed in LCO 3.7.2, "Control Room Habitability Area (CRHA) Heating, Ventilation, and Air Conditioning (HVAC) Subsystem (CRHAVS)."

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

The ability of the CRHAVS to maintain habitability of the CRHA is an explicit assumption for the safety analyses presented in Chapter 6 and Chapter 15, (Refs. 1 and 3, respectively). The isolation mode of the CRHAVS is assumed to operate following a design basis accident (DBA). The radiological dose to control room personnel as a result of various DBAs is summarized in Reference 3. No single active failure will result in a loss of the system design function.

CRHAVS instrumentation satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

The OPERABILITY of the CRHAVS instrumentation is dependent on the OPERABILITY of the individual instrumentation channel Functions specified in Table 3.3.7.1-1. Each Function must have the required number of OPERABLE channels, with their setpoints in accordance with the SCP, where appropriate.

$NTSP_F$s are specified in the SCP, as required by Specification 5.5.11. The $NTSP_F$s are conservative with respect to the Allowable Value between successive CHANNEL CALIBRATIONS. Operation with a trip setpoint less conservative than the $NTSP_F$, but conservative with respect to its Allowable Value, is acceptable. A channel is inoperable if its actual trip setpoint is non-conservative with respect to its required Allowable Value.

The individual Functions are required to be OPERABLE in MODES 1, 2, 3, and 4 to maintain habitability of the control room following a DBA, since the DBA could lead to a fission product release.

In MODES 5 and 6, the probability and consequences of a DBA are reduced due to the pressure and temperature limitations in these MODES. Therefore, the Functions listed in Table 3.3.7.1-1 are not required to be OPERABLE in MODES 5 or 6, except for other situations under which significant radioactive releases can be postulated, i.e., during operations with a potential for draining the reactor vessel (OPDRVs).

Although there are four channels of CRHAVS instrumentation for each function, only three channels of CRHAVS instrumentation for each function are required to be OPERABLE. The three required channels are those channels associated with the DC and Uninterruptible AC Electrical Power Distribution Divisions required by LCO 3.8.6, "Distribution Systems – Operating," and LCO 3.8.7, "Distribution Systems – Shutdown." This is acceptable because the single-failure criterion is met with three

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

OPERABLE CRHAVS instrumentation channels, and because each CRHAVS instrumentation division is associated with and receives power from only one of the four electrical divisions.

The specific Applicable Safety Analyses, LCO and Applicability discussions are listed below on a Function-by-Function basis.

1. Control Room Air Intake Radiation – High-High

Radiation monitors for the Control Building Air Intake consist of four redundant channels to monitor the air intake to the building. Each radiation channel consists of a gamma sensitive detector and a radiation monitor that is located in the main control room.

The Control Room Air Intake Radiation – High-High Allowable Value is chosen to ensure the control room is isolated prior to exceeding the 10 CFR 50 Appendix A GDC 19 requirements.

Three channels of Control Room Air Intake Radiation – High-High Function are required to be OPERABLE to ensure no single instrument failure will preclude CRHA isolation and actuation of CRHAVS in the emergency filtration mode of operation.

2. Extended Loss of AC Power

If the nonsafety-related main air supply units are de-energized due to a loss of AC power, the SSLC/ESF provides an initiation signal as a conservative measure assuming a radiological release.

Three channels of Extended Loss of AC Power Function are required to be OPERABLE to ensure no single instrument failure will preclude CRHA isolation and actuation of CRHAVS in the emergency filtration mode of operation.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

3. EFU Discharge Flow – Low (primary train)

Flow detectors for the EFU outlets consist of four redundant channels on each filter train to monitor the flow rate of filtered air being supplied to the Control Room Habitability Area. When low flow is detected and has not been corrected by start of the operating train's standby EFU fan, then the standby EFU train automatically starts to continue the emergency filtration mode. Any two-out-of-four channel trips result in the automatic shutdown of the in-service EFU and automatic start-up of the standby EFU.

The EFU Discharge Flow - Low Allowable Value is chosen to ensure swap over of the EFU such that the control room remains pressurized.

Three channels of EFU Discharge Flow - Low Function for the selected primary CRHAVS train are required to be OPERABLE to ensure no single instrument failure will preclude actuation of the standby CRHAVS train in the emergency filtration mode of operation.

4. EFU Outlet Radiation – High-High (primary train)

Radiation monitors for the EFU outlets consist of four redundant channels on each filter train to monitor the filtered air to the Control Room Habitability Area. Each radiation channel consists of a gamma sensitive detector and a radiation monitor that is located in the main control room. Any two-out-of-four channel trips result in the automatic shutdown of the in-service EFU and automatic start-up of the standby EFU.

The EFU Outlet Radiation – High-High Allowable Value is chosen to ensure swap over of the EFU without exceeding the 10 CFR 50 Appendix A GDC 19 requirements.

Three channels of EFU Outlet Radiation – High-High Function for the selected primary CRHAVS train are required to be OPERABLE to ensure no single instrument failure will preclude actuation of the standby CRHAVS train in the emergency filtration mode of operation.

BASES

ACTIONS

The ACTIONS have been modified by a Note to permit separate Condition entry for each CRHAVS instrumentation channel. Section 1.3, Completion Times, specifies once a Condition has been entered, subsequent divisions, subsystems, components or variables expressed in the Condition discovered to be inoperable or not within limits, will not result in separate entry into the Condition. Section 1.3 also specifies Required Actions of the Condition continue to apply for each additional failure, with Completion Times based on initial entry into the Condition. However, the Required Actions for inoperable CRHAVS instrumentation channels provide appropriate compensatory measures for separate inoperable Condition entry for each inoperable CRHAVS instrumentation channel.

A.1

With one or more Functions with one required channel inoperable, the required channel must be restored to Operable status within 12 hours.

The 12-hour Completion Time is acceptable based on engineering judgment considering the diversity of sensors available to provide actuation signals, the redundancy of the CRHAVS instrumentation design, and the low probability of an event requiring CRHAVS actuation during this period.

However, this out of service time is only acceptable provided the associated Function still maintains CRHAVS actuation capability (refer to Required Actions B.1 Bases).

Alternatively, if the instrumentation division can not be restored to OPERABLE status, Condition B must be entered and its Required Action taken when the Completion Time of Required Action A.1 expires.

B.1

Required Action B.1 directs entry into the appropriate Condition referenced in Table 3.3.7.1-1 if the Required Action and Completion Time of Condition A is not met or if multiple, inoperable, untripped required channels for the same Function result in the Function not maintaining CRHAVS actuation capability. A Function is considered to be maintaining CRHAVS actuation capability when sufficient channels are OPERABLE or in trip such that the CRHAVS logic will generate an initiation signal from the given Function on a valid signal. The applicable Condition specified in the Table is Function dependent.

BASES

ACTIONS (continued)

C.1.1, C.1.2, and C.2

If the required channel(s) is not restored to OPERABLE status within the allowed Completion Time or if CRHAVS actuation capability for the Function is not maintained, the associated feature(s) may be incapable of performing the intended function.

Required Action C.1.1 and Required Action C.1.2 require manual isolation of the CRHA boundary and placing an OPERABLE CRHAVS train in the isolation mode, respectively, which accomplishes the safety function by ensuring radiological protection of the occupants within the CRHA boundary.

Alternatively, Required Action C.2 requires declaring the CRHAVS trains inoperable in accordance with LCO 3.7.2. Declaring the CRHAVS trains inoperable is acceptable, since the Required Actions of LCO 3.7.2 provide appropriate actions for the inoperable components

D.1

If the required channel(s) is not restored to OPERABLE status within the allowed Completion Time or if CRHAVS actuation capability for the Function is not maintained, the signal(s) to automatically swap CRHAVS trains may be incapable of performing the intended function and the affected CRHAVS train (the standby train) must be declared inoperable immediately.

SURVEILLANCE REQUIREMENTS

The SRs are modified by a Note. The Note directs the reader to Table 3.3.7.1-1 to determine the correct SRs to perform for each CRHAVS Function.

SR 3.3.7.1.1

Performance of the CHANNEL CHECK once every 12 hours ensures that a gross failure of instrumentation has not occurred.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The SSLC/ESF is cyclically tested from the sensor input point to the logic contact output by online self-diagnostics. The self-diagnostic capabilities include microprocessor checks, system initialization, watchdog timers, memory integrity checks, input/output (I/O) data integrity checks and communication bus interface checks, and checks on the application program (checksum).

A CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

Agreement criteria are determined by the plant staff, based on a combination of the channel instrument uncertainties, including indication and readability. If a channel is outside the criteria, it may be an indication that the instrument has drifted outside its limit.

The Frequency is based upon operating experience that demonstrates channel failure is rare. The CHANNEL CHECK every 12 hours supplements less formal, but more frequent, checks of channels during normal operational use of the displays associated with the channels required by the LCO.

SR 3.3.7.1.2

A CHANNEL FUNCTIONAL TEST is performed on each required channel to ensure that the entire channel will perform the intended function. This test ensures a complete CHANNEL FUNCTIONAL TEST of required instrument channels from the sensor input through the DTM function.

The SSLC/ESF is cyclically tested from the sensor input point to the logic contact output by online self-diagnostics. The self-diagnostic capabilities include microprocessor checks, system initialization, watchdog timers, memory integrity checks, input/output (I/O) data integrity checks and communication bus interface checks, and checks on the application program (checksum).

The Frequency of 31 days is based on the reliability of the CRHAVS instrumentation channels.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.7.1.3

A CHANNEL CALIBRATION is a complete check of the instrument loop and the sensor. This test verifies the required channel responds to the measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the required channel adjusted to the $NTSP_F$ within the "as-left" tolerance to account for instrument drifts between successive calibrations consistent with the methods and assumptions required by the SCP.

The Frequency is based upon the assumption of a 24-month calibration interval in the determination of the magnitude of equipment drift in the setpoint.

SR 3.3.7.1.4

This SR ensures that the individual required channel response times are less than or equal to the maximum values assumed in the accident analysis. The instrument response times must be added to the associated closure times to obtain the CRHAVS RESPONSE TIME. CRHAVS RESPONSE TIME acceptance criteria are included in Reference 4.

CRHAVS RESPONSE TIME may be verified by actual response time measurements in any series of sequential, overlapping, or total channel measurements. This test encompasses the isolation instrumentation from the input variable sensors through the DTM function.

This test overlaps the testing required by SR 3.3.7.2.2 to ensure complete testing of instrumentation channels and actuation circuitry.

A Note to the Surveillance states that the radiation detectors may be excluded from CRHAVS RESPONSE TIME testing. This Note is necessary because of the difficulty of generating an appropriate detector input signal and because the principles of detector operation virtually ensure an instantaneous response time. Response Time for radiation detection channels shall be measured from detector output or the input of the first electronic component in the channel.

BASES

SURVEILLANCE REQUIREMENTS (continued)

COL 16.0-1-A
3.3.7.1-3

[However, some sensors are allowed to be excluded from specific CRHAVS RESPONSE TIME measurement if the conditions of Reference XX are satisfied. If these conditions are satisfied, sensor response time may be allocated based on either assumed design sensor response time or the manufacturer's stated design response time. When the requirements of Reference XX are not satisfied, sensor response time must be measured. Furthermore, measurement of the instrument loops response time for some Functions is not required if the conditions of Reference XX are satisfied.]

CRHAVS RESPONSE TIME tests are conducted on a 24-month STAGGERED TEST BASIS for three channels. The Frequency of 24 months on a STAGGERED TEST BASIS ensures that the channels associated with each division are alternately tested. The 24-month test Frequency is consistent with the refueling cycle and with operating experience that shows that random failures of instrumentation components causing serious response time degradation, but not channel failure, are infrequent.

REFERENCES

1. Section 6.4.
2. Section 9.4.1.
3. Section 15.4.
4. Section 15.2.

B 3.3 INSTRUMENTATION

B 3.3.7.2 Control Room Habitability Area (CRHA) Heating, Ventilation, and Air Conditioning (HVAC) Subsystem (CRHAVS) Actuation

BASES

BACKGROUND

The purpose of the CRHAVS actuation logic is to initiate appropriate actions to ensure the CRHAVS and control room habitability area (CRHA) boundary provide a protected environment from which occupants can control the unit following an uncontrolled release of radioactivity [hazardous chemicals]. The equipment involved with CRHAVS is described in the Bases for LCO 3.7.2, "Control Room Habitability Area (CRHA) Heating, Ventilation, and Air Conditioning (HVAC) Subsystem (CRHAVS)."

COL 16.0-1-A 3.3.7.2-1

This specification addresses OPERABILITY of the CRHAVS actuation circuitry from the outputs of the Digital Trip Module (DTM) functions through the voter logic unit (VLU) functions and the load drivers (LDs) associated with the CRHAVS. Operability requirements associated with the CRHAVS instrumentation channels are provided in LCO 3.3.7.1, "Control Room Habitability Area (CRHA) Heating, Ventilation, and Air Conditioning (HVAC) Subsystem (CRHAVS) Instrumentation." Operability requirements for actuated components (i.e., dampers and valves) are addressed in LCO 3.7.2, "Control Room Habitability Area (CRHA) Heating, Ventilation, and Air Conditioning (HVAC) Subsystem (CRHAVS)."

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

The ability of the CRHAVS to maintain habitability of the CRHA is an explicit assumption for the safety analyses presented in Chapter 6 and Chapter 15, (Refs. 1 and 2, respectively). The isolation mode of the CRHAVS is assumed to operate following a design basis accident (DBA). The radiological dose to control room occupants as a result of various DBAs is summarized in Reference 2. No single active failure will result in a loss of the system design function.

CRHAVS actuation satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

CRHAVS actuation supports OPERABILITY of the CRHAVS Instrumentation, LCO 3.3.7.1, "Control Room Habitability Area (CRHA) Heating, Ventilation, and Air Conditioning (HVAC) Subsystem (CRHAVS) Instrumentation," and therefore is required to be OPERABLE. This Specification addresses OPERABILITY of the CRHAVS actuation circuitry from the outputs of the DTM functions through the LDs, which covers the VLU functions and the LDs associated with the CRHA isolation dampers, CRHAVS Emergency Filtration Unit (EFU) fans and isolation dampers, and Nonsafety-Related Distributed Control and Information System (N-DCIS) electrical load breakers, and other nonsafety-related electrical loads in the CRHA.

Although there are four divisions of CRHAVS actuation, only three CRHAVS actuation divisions are required to be OPERABLE. The three required divisions are those divisions associated with the DC and Uninterruptible AC Electrical Power Distribution Divisions required by LCO 3.8.6, "Distribution Systems – Operating," and LCO 3.8.7, "Distribution Systems – Shutdown." This is acceptable because the single-failure criterion is met with three OPERABLE CRHAVS actuation divisions, and because each CRHAVS actuation division is associated with and receives power from only one of the four electrical divisions.

In MODES 1, 2, 3, and 4 the CRHAVS must be OPERABLE to maintain habitability of the control room following a DBA, since the DBA could lead to a fission-product release.

In MODES 5 and 6, the probability and consequences of a DBA are reduced due to the pressure and temperature limitations in these MODES. Therefore, maintaining the CRHAVS OPERABLE is not required in MODE 5 or 6, except for other situations under which significant radioactive releases can be postulated, i.e., during operations with a potential for draining the reactor vessel (OPDRVs).

BASES

ACTIONS

A.1

Condition A exists when one required CRHAVS actuation division is inoperable. In this Condition, CRHAVS actuation still maintains actuation trip capability, but cannot accommodate a single failure. The 12-hour Completion Time is acceptable based on engineering judgment considering the diversity of sensors available to provide trip signals, the redundancy of the CRHAVS actuation design, and the low probability of an event requiring CRHAVS actuation during this period. However, this out of service time is only acceptable provided the associated Function still maintains CRHAVS actuation capability (refer to Required Actions B.1.1, B.1.2, B.1.3, and B.2 Bases).

Alternatively, if it is not desired to restore the required actuation division to OPERABLE status, Condition B must be entered and its Required Action taken when the Completion Time of Required Action A.1 expires.

B.1.1, B.1.2, B.1.3, and B.2

With the Required Actions and associated Completion Times of Condition A or B are not met, or two or more required actuation divisions are inoperable, the associated feature(s) may be incapable of performing the intended function. CRHAVS automatic actuation capability is considered to be maintained when sufficient actuation divisions are OPERABLE or in trip such that the CRHAVS logic will generate an actuation signal on a valid signal.

Required Action B.1.1 and Required Action B.1.2 require manual isolation of the CRHA boundary and placing an OPERABLE CRHAVS train in the isolation mode, respectively, which accomplishes the safety function of the inoperable channel by ensuring radiological protection of the occupants within the CRHA boundary. Required Action B.1.3 requires declaring the CRHAVS train that is not placed in service inoperable since a failure in the actuation division may affect its ability to initiate upon a failure of the in-service train. Declaring the remaining CRHAVS train inoperable is acceptable, since the Required Actions of LCO 3.7.2 provide appropriate actions for the inoperable train.

Alternatively, Required Action B.2 requires declaring the affected actuation device(s) inoperable in accordance with LCO 3.7.2. Declaring the affected actuation device(s) inoperable is acceptable, since the Required Actions of LCO 3.7.2 provide appropriate actions for the inoperable components.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.3.7.2.1

The LOGIC SYSTEM FUNCTIONAL TEST demonstrates the OPERABILITY of the required CRHAVS logic for a specific division.

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 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 24-month Frequency.

SR 3.3.7.2.2

This SR ensures that the individual required division response times are less than or equal to the maximum values assumed in the accident analysis. The instrument response times must be added to the associated closure times to obtain the CRHAVS RESPONSE TIME. CRHAVS RESPONSE TIME acceptance criteria are included in Reference 3.

CRHAVS RESPONSE TIME may be verified by actual response time measurements in any series of sequential, overlapping, or total channel measurements. This test encompasses the isolation actuation circuitry consisting of timers, VLU functions, and load drivers. This test overlaps the testing required by SR 3.3.7.1.4 to ensure complete testing of instrumentation channels and actuation divisions.

COL 16.0-1-A 3.3.7.2-2

[However, some portions of the isolation actuation circuitry are allowed to be excluded from specific CRHAVS RESPONSE TIME measurement if the conditions of Reference XX are satisfied. Furthermore, measurement of the instrument loops response time for some Functions is not required if the conditions of Reference XX are satisfied.]

CRHAVS RESPONSE TIME tests are conducted on a 24-month STAGGERED TEST BASIS for three divisions. The Frequency of 24 months on a STAGGERED TEST BASIS ensures that the channels associated with each division are alternately tested. The 24-month test Frequency is consistent with the refueling cycle and with operating experience that shows that random failures of instrumentation components causing serious response time degradation, but not channel failure, are infrequent.

BASES

REFERENCES	1.	Section 6.4.
	2.	Section 15.4.
	3.	Section 15.2.

B 3.3 INSTRUMENTATION

B 3.3.8.1 Diverse Protection System (DPS)

BASES

BACKGROUND

The DPS comprises a portion of the diverse instrumentation and control systems that are part of the diversity and defense-in-depth strategy.

The DPS functions are implemented in the Nonsafety-Related Distributed Control and Information System (N-DCIS) as a highly reliable, triple redundant control system whose sensors, hardware and software are diverse from their counterparts on any of the safety-related instrumentation and control systems. The DPS is a nonsafety-related, triple redundant system powered by redundant nonsafety-related load group power supplies.

DPS provides a set of initiation logics that provide a diverse means to initiate certain engineered safety feature (ESF) functions using sensors, hardware and software that are separate from, and independent of, the primary ESF systems. The ESF Functions include core cooling provided by the Gravity-Driven Cooling System (GDCS) and the Automatic Depressurization System (ADS) function using safety relief valves (SRVs) and depressurization valves (DPVs). The initiating logic is based on Reactor Pressure Vessel Level – Low, Level 1.

The initiation logic is "energize to actuate," similar to that described in the Bases for LCO 3.3.5.1, " Emergency Core Cooling System (ECCS) Instrumentation," and LCO 3.3.5.2, " Emergency Core Cooling System (ECCS) Actuation." The diverse ECCS automatic initiation signal is based on two-out-of-four coincident logic processed by triple redundant processors. If the DPS ECCS initiation signal persists for 10 seconds, the logic seals in and a DPS ECCS start signal is initiated. Manual initiation requires operation of two switches, with each switch requiring two distinct operator actions. The manual initiation signal is based on two-out-of-two coincident logic processed by triple redundant processors. A coincident logic trip decision is required from two-out-of-three processors to generate the start signal. Series discrete output switches independently process the two-out-of-three voted start signal. A valid initiation signal from all series output switches is required to generate diverse actuation.

BASES

BACKGROUND (continued)

For the ADS SRV opening function, three of the four solenoids on each SRV are powered by three of the four divisional safety-related power sources in the Safety System Logic and Control Engineered Safety Features (SSLC/ESF) ADS described in the Bases for LCO 3.3.5.1 and LCO 3.3.5.2. A fourth solenoid on each SRV is powered by the nonsafety-related load group, with the trip logic controlled by DPS. All ten SRVs in the ADS are controlled by the DPS through the fourth solenoid on each valve.

For the ADS DPV opening function, one of the four squib initiators on each DPV is controlled by and connected to the nonsafety-related DPS logic. The other three solenoids are controlled by the SSLC/ESF ADS logic described in the Bases for LCO 3.3.5.1 and LCO 3.3.5.2. It takes three simultaneous DPS trip signals in a triple redundant logic path to initiate the squib valve opening.

The logic application for the GDCS squib valves from the DPS is similar to that of the DPV logic application described above. For the GDCS squib valve-opening function, one of the four squib initiators on each GDCS valve is controlled by and connected to the nonsafety-related DPS logic. The DPS logic requires three simultaneous GDCS trip initiation signals to initiate a GDCS squib valve opening.

The DPS also performs selected containment isolation functions as part of the diverse ESF function using two-out-of-four sensor logic and two-out-of-three processing logic. The containment isolation functions performed by DPS include closure of the Reactor Water Cleanup and Shutdown Cooling (RWCU/SDC) isolation valves on Reactor Water Cleanup/Shutdown Cooling System Differential Mass Flow – High.

The DPS also opens pool cross-connect valves between the equipment storage pool and the Isolation Condenser/Passive Containment Cooling System (IC/PCCS) expansion pools when a low level condition is detected in the IC/PCCS inner expansion pool to which the valves are connected. Each IC/PCCS pool is connected to the equipment storage pool by two cross-connect valves in parallel where one valve is a pneumatic operated valve with an accumulator and the other is a squib valve. Each expansion pool-to-equipment pool cross-connect squib valve is equipped with four squib initiators. The expansion pool-to-equipment pool cross-connect pneumatic valves are equipped with four solenoid valves (i.e., initiators). A signal to any of the four initiators will actuate the valve. One of the four initiators on each valve is actuated by DPS.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY	The DPS Functions are required to provide a diverse capability to actuate the specified safety-related equipment based on risk importance (Ref. 1). The DPS Functions are not credited for mitigating accidents in the safety analyses (Ref. 2). The DPS satisfies Criterion 4 of 10 CFR 50.36(c)(2)(ii).

Each Function must have its setpoint in accordance with the Setpoint Control Program (SCP), where appropriate. The actual setpoint is calibrated consistent with the SCP.

Nominal Trip Setpoints ($NTSP_F$s) are specified in the Setpoint Control Program (SCP), as required by Specification 5.5.11. The $NTSP_F$s are selected to ensure the actual setpoints are conservative with respect to the Allowable Value between successive CHANNEL CALIBRATIONS. Operation with a trip setpoint less conservative than the $NTSP_F$, but conservative with respect to its Allowable Value, is acceptable. A Function is inoperable if its actual trip setpoint is non-conservative with respect to its required Allowable Value.

$NTSP_F$s are those predetermined values of output at which an action should take place. The setpoints are compared to the actual process parameter (e.g., reactor vessel water level), and when the measured output value of the process parameter exceeds the setpoint, an actuation signal is generated. For those limiting safety system settings (LSSS) related to variable protecting Safety Limits (SLs), the Analytical Limits are derived from the limiting values of the process parameters obtained from the safety analysis. For those LSSS related to variables having significant safety functions but which do not protect SLs, the Design Limits are those settings that must initiate automatic protective actions consistent with the design basis. The Allowable Values are derived from the Analytical / Design Limits, corrected for calibration, process and some of the instrument errors. The $NTSP_F$s are then determined accounting for the remaining instrument errors (e.g., drift). The trip setpoints derived in this manner provide adequate protection because instrumentation uncertainties, process effects, calibration tolerances, instrument drift and severe environment errors (for instrumentation that must function in harsh environments as defined by 10 CFR 50.49) are accounted for.

The specific Applicable Safety Analyses, LCO, and Applicability discussions are listed below on a Function-by-Function basis.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

1.a, 2.a Reactor Vessel Level – Low, Level 1

Automatic actuation of ADS (consisting of the SRVs and DPVs) and GDCS injection occurs upon detection of Reactor Vessel Level – Low, Level 1. Reactor Vessel water level is detected by four wide range water level sensors that are different from those used for the SSLC/ESF wide range level sensors. Low RPV water level indicates the capability to cool the fuel may be threatened. Should RPV water level decrease too far, fuel damage could result.

The Reactor Vessel Level – Low, Level 1 Function is required to be OPERABLE in MODES 1, 2, 3, and 4, consistent with the assumptions in Reference 1.

1.b, 2.b Drywell Pressure – High (Manual Actuation)

Manual controls are provided for ADS (consisting of the SRVs and DPVs) and GDCS injection initiation upon detection of high drywell pressure sustained for 60 minutes. This control is provided to mitigate small and medium break LOCA scenarios that do not result in GDCS and ADS initiation from low RPV water level. This Function also requires OPERABILITY of DPS indication of the high drywell pressure condition.

The Drywell Pressure – High (Manual Actuation) Function is required to be OPERABLE in MODES 1, 2, 3, and 4 consistent with the assumptions in Reference 1.

3.a. Reactor Vessel Level – Low (Manual Actuation)

Manual controls are provided for initiation of the GDCS equalizing lines upon detection of low reactor vessel water level. Low RPV water level indicates the capability to cool the fuel may be threatened. Should RPV water level decrease too far, fuel damage could result. This Function also requires OPERABILITY of DPS indication of the low water level condition.

The Reactor Vessel Level – Low (Manual Actuation) Function is required to be OPERABLE in MODES 1, 2, 3, and 4, consistent with the assumptions in Reference 1.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

4.a Reactor Water Cleanup/Shutdown Cooling System Differential Mass Flow – High

Automatic isolation of RWCU/SDC occurs upon detection of Reactor Water Cleanup/Shutdown Cooling System Differential Mass Flow – High. Isolation of the RWCU System is initiated when RWCU/SDC System Differential Mass Flow – High is sensed to prevent exceeding off-site doses.

The function of the RWCU/SDC isolation valves, in combination with other accident mitigation systems, is to limit fission product release during a postulated Design Bases Accident (DBA).

The Reactor Water Cleanup/Shutdown Cooling System Differential Mass Flow – High Function is required to be OPERABLE in MODES 1, 2, 3, and 4, consistent with the assumptions in Reference 1.

5.a Isolation Condenser/Passive Containment Cooling System Pool Level – Low

Automatic actuation of the IC/PCCS expansion pool-to-equipment pool cross-connect occurs upon detection of Isolation Condenser/Passive Containment Cooling System Pool Level – Low in the associated IC/PCCS inner expansion pool. Actuation of the IC/PCCS expansion pool-to-equipment pool cross-connect ensures a sufficient quantity of water is available for decay heat removal in the event of a design basis accident.

The Isolation Condenser/Passive Containment Cooling System Pool Level – Low Function is required to be OPERABLE in MODES 1, 2, 3, and 4, consistent with the assumptions in Reference 1.

ACTIONS

A Note has been provided to modify the ACTIONS related to the DPS Functions. Section 1.3, Completion Times, specifies once a Condition has been entered, subsequent divisions, subsystems, components or variables expressed in the Condition discovered to be inoperable or not within limits, will not result in separate entry into the Condition. Section 1.3 also specifies Required Actions of the Condition continue to apply for each additional failure, with Completion Times based on initial entry into the condition. However, the Required Actions for inoperable DPS Functions provide appropriate compensatory measures for separate

BASES

ACTIONS (continued)

inoperable Functions. As such, a Note has been provided which allows separate Condition entry for each inoperable DPS Function.

A.1

In this Condition, required safety-related initiators will actuate the components assumed in the design basis LOCA analysis in Reference 2 concurrent with any additional single failure. However, design features intended to mitigate digital protection system common mode failures may not be available.

In this Condition, the inoperable Function must be restored to OPERABLE status within 30 days. This Completion Time is acceptable because the required safety-related initiators will actuate the minimum number of components required to respond to the design basis LOCA concurrent with any additional single failure.

B.1 and B.2

With the Required Action and associated Completion Time of Condition A not met, 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 12 hours and to MODE 5 within 36 hours. The Completion Time is reasonable, based on plant design, to reach required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.3.8.1.1

Performance of the CHANNEL CHECK once every 12 hours ensures that a gross failure of DPS has not occurred. The associated controllers, displays, monitoring and input/output (I/O) communication interfaces continuously function during normal power operation. Abnormal operation of these components is detected and alarmed. In addition, the associated controllers are equipped with on-line diagnostic capabilities for cyclically monitoring the functionality of I/O signals, buses, power supplies, processors, and inter-processor communications.

A CHANNEL CHECK will detect gross DPS failure; thus, it is key to verifying the DPS continues to operate properly between each CHANNEL CALIBRATION.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The Frequency is based upon operating experience that demonstrates failure of the DPS components is rare. The CHANNEL CHECKS every 12 hours supplement less formal, but more frequent checks of DPS during normal operational use of the displays associated with the Functions required to be OPERABLE by the LCO.

SR 3.3.8.1.2

A CHANNEL FUNCTIONAL TEST is performed on the DPS to ensure that the entire DPS will perform the intended Functions. The associated controllers, displays, monitoring and input/output (I/O) communication interfaces continuously function during normal power operation. Abnormal operation of these components is detected and alarmed. In addition, the associated controllers are equipped with on-line diagnostic capabilities for cyclically monitoring the functionality of I/O signals, buses, power supplies, processors, and inter-processor communications.

The 31-day Frequency is based on the reliability of the DPS.

SR 3.3.8.1.3

A CHANNEL CALIBRATION is a complete check of the instrument loop and the sensor. This test verifies the DPS responds to the measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the DPS adjusted to the $NTSP_F$ within the "as-left" tolerance to account for instrument drifts between successive calibrations consistent with the methods and assumptions required by the SCP.

The Frequency is based upon the assumption of a 24-month calibration interval in the determination of the magnitude of equipment drift in the setpoint analysis.

SR 3.3.8.1.4

The LOGIC SYSTEM FUNCTIONAL TEST demonstrates the OPERABILITY of the DPS logic. LOGIC SYSTEM FUNCTIONAL tests are conducted on a 24-month Frequency. The testing in LCO 3.3.6.4, "Isolation Actuation," LCO 3.6.1.3, "Containment Isolation Valves (CIVs)," LCO 3.5.2, “Gravity-Driven Cooling System (GDCS) – Operating,” and LCO 3.7.1, "Isolation Condenser/Passive Containment Cooling

BASES

SURVEILLANCE REQUIREMENTS (continued)

System (IC/PCCS) Pools," overlaps this Surveillance to provide complete testing of the assumed safety function.

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 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 24-month Frequency.

REFERENCES

1. Chapter 19.
2. Chapter 15.

B 3.4 REACTOR COOLANT SYSTEM (RCS)

B 3.4.1 Safety Relief Valves (SRVs)

BASES

BACKGROUND	The American Society of Mechanical Engineers (ASME) Boiler and Pressure Vessel Code (Ref. 1) requires the Reactor Pressure Vessel be protected from overpressure during upset conditions by self-actuated safety valves. As part of the nuclear pressure relief system, the size and number of SRVs are selected such that peak pressure in the nuclear system will not exceed the ASME Code limits for the reactor coolant pressure boundary (RCPB). The ESBWR steam relief capacity is designed to satisfy both ASME Code Service Level B (upset) overpressure protection, and Service Level C (emergency) design service limits (Ref. 2). This LCO addresses only those requirements for operability of the vessel overpressure protection that satisfy the Service Level B pressure limits. The SRVs are located on the main steam lines between the reactor vessel and the first isolation valve within the drywell. In the safety mode, the direct action of the steam pressure in the main steam lines will act against a spring-loaded disk that will pop open when the valve inlet pressure exceeds the spring force and the frictional forces acting against the inlet steam pressure at the main or pilot disk.
APPLICABLE SAFETY ANALYSES	The overpressure protection system must accommodate the most severe pressure transient. Evaluations have determined that the most severe Service Level B pressure transient is the closure of all main steam isolation valves (MSIVs) followed by reactor scram on high neutron flux (i.e., failure of the direct scram associated with MSIV position) (Ref. 3). The analysis results demonstrate that the design capacity of one SRV is capable of maintaining reactor pressure below the ASME Code limit of 110% of vessel design pressure, i.e., 110% x 8.62 MPaG (1250 psig) = 9.48 MPaG (1375 psig). This LCO helps to ensure that the acceptance limit of 9.48 MPaG (1375 psig) is met during the design basis event. From an overpressure standpoint, the design basis events are bounded by the MSIV closure with flux scram event described above. Reference 4 discusses additional events that are expected to actuate the SRVs. Safety relief valves satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO

The results of the overpressure analysis provided in Reference 3 demonstrate that one SRV is required to function in the safety mode to meet ASME overpressure protection. Therefore, to satisfy the design basis overpressure event (including provision for single failure), two SRVs are required to be OPERABLE. The requirements of this LCO are applicable only to the capability of the SRVs to mechanically open in the safety mode to relieve excess pressure.

The SRV setpoints are established to ensure the ASME Code limit on peak reactor pressure is satisfied. The ASME Code specifications require the lowest safety valve be set at or below vessel design pressure, i.e., 8.62 MPaG (1250 psig), and the highest safety valve is set so the total accumulated pressure does not exceed 110% of the design pressure for conditions. The transient evaluations in Reference 3 assume that the SRV setpoints are at conservatively high values above the nominal setpoints to account for initial setpoint errors and any setpoint drift that might occur during operation.

Operation with fewer valves OPERABLE than specified, or with setpoints greater than specified, could result in a more severe reactor response to a transient than predicted, possibly resulting in the ASME Code limit on reactor pressure being exceeded.

APPLICABILITY

In MODES 1, 2, 3 and 4, the specified number of SRVs must be OPERABLE because there may be considerable energy in the reactor core and the limiting design basis transients are assumed to occur.

In MODE 5, reactor pressure is low enough that the overpressure limit is not likely to be approached by assumed operational transients or accidents. In MODE 6, the reactor vessel head is unbolted or removed and the reactor is at atmospheric pressure. Therefore, the SRV function is not required by LCO 3.4.1 during these conditions.

ACTIONS

A.1

With the safety mode of one required SRV inoperable, the remaining operable SRV is capable of providing the necessary overpressure protection. However, the overall reliability of the pressure relief system is reduced because additional failure of the remaining OPERABLE SRV could result in failure to adequately relieve pressure during an overpressure event. For this reason, continued operation is permitted for a limited time only.

BASES

ACTIONS (continued)

The 14-day Completion Time to restore the inoperable required SRV to OPERABLE status is based on the relief capability of the remaining SRV, the low probability of an event requiring SRV actuation, and a reasonable time to complete the Required Action.

B.1

If the Required Action and associated Completion Time of Condition A cannot be met, or with less than the minimum number of required SRVs OPERABLE, 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 12 hours and MODE 5 within 36 hours. The Completion Time is reasonable, based on plant design, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.4.1.1

This Surveillance demonstrates that the required SRVs will open at the pressures assumed in the safety analysis of Reference 3.

The demonstration of the SRV safety mode lift settings is a bench test and must be performed during shutdown. The SRV setpoint is ± 3% for OPERABILITY and the valves are reset to ± 1% during the Surveillance.

The Frequency of this SR is in accordance with the Inservice Testing Program.

REFERENCES

1. ASME, Boiler and Pressure Vessel Code, Section III.
2. Section 5.2.2.
3. Section 15.5.1.
4. Section 15.5.4

B 3.4 REACTOR COOLANT SYSTEM (RCS)

B 3.4.2 RCS Operational LEAKAGE

BASES

BACKGROUND

The RCS includes systems and components that contain or transport the coolant to or from the reactor core. The pressure containing components of the RCS and the portions of connecting systems out to and including the isolation valves define the reactor coolant pressure boundary (RCPB). The joints of the RCPB components are welded unless applicable codes permit flanged or threaded joints.

During plant life, the joint and valve interfaces can produce varying amounts of reactor coolant LEAKAGE, through either normal operational wear or mechanical deterioration. Limits on RCS operational LEAKAGE are required to ensure appropriate action is taken before the integrity of the RCPB is impaired. This LCO specifies the types and limits of LEAKAGE.

This protects the RCS pressure boundary described in 10 CFR 50.2, 10 CFR 50.55a(c) and GDC 55 of 10 CFR 50, Appendix A (Ref. 1, 2, and 3). 10 CFR 50, Appendix A, GDC 30 (Ref. 4), requires means for detecting and, to the extent practical, identifying the source of reactor coolant LEAKAGE. Regulatory Guide 1.45 (Ref. 5) describes acceptable methods for selecting Leakage Detection Systems.

The safety significance of leaks from the RCPB varies widely depending on the source, rate, and duration. Therefore, detection of LEAKAGE in the primary containment is necessary. Methods for quickly separating the identified LEAKAGE from the unidentified LEAKAGE are necessary to provide the operators quantitative information to permit them to take corrective action should a leak occur detrimental to the safety of the facility or the public.

A limited amount of leakage inside primary containment is expected from auxiliary systems that cannot be made 100% leak tight. Leakage from these systems should be detected and isolated from the primary containment atmosphere, if possible, so as not to mask RCS operational LEAKAGE detection.

BASES

BACKGROUND (continued)

This LCO deals with protection of the RCPB from degradation and the core from inadequate cooling, in addition to preventing the accident analyses radiation release assumptions from being exceeded. The consequences of violating this LCO include the possibility of a loss-of-coolant accident.

APPLICABLE SAFETY ANALYSES

The allowable RCS operational LEAKAGE limits are based on the predicted and experimentally observed behavior of pipe cracks. The normally expected background LEAKAGE due to equipment design and the detection capability of the instrumentation for determining system LEAKAGE were also considered. The evidence from experiments suggests, for LEAKAGE even greater than the specified unidentified LEAKAGE limits, the probability is small that the imperfection or crack associated with such LEAKAGE would grow rapidly.

The unidentified LEAKAGE flow limit allows time for corrective action before the RCPB could be significantly compromised. The allowable LEAKAGE limits are based on the predicted and experimentally determined behavior of cracks in pipes, the ability to makeup to the RCS, the normally expected background leakage due to equipment design, and the detection capability of the various sensors and instruments.

No applicable safety analysis assumes the total LEAKAGE limit. The total LEAKAGE limit considers RCS inventory makeup capability and drywell floor sump capacity.

RCS operational LEAKAGE satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

RCS operational LEAKAGE shall be limited to:

a. Pressure Boundary LEAKAGE

No pressure boundary LEAKAGE is allowed, being indicative of material degradation. LEAKAGE of this type is unacceptable as the leak itself could cause further deterioration, resulting in higher LEAKAGE. Violation of this LCO could result in continued degradation of the RCPB. LEAKAGE past seals and gaskets are not pressure boundary LEAKAGE.

BASES

LCO (continued)

b. Unidentified LEAKAGE

The unidentified LEAKAGE limit is based on a reasonable minimum detectable amount that the drywell air monitoring, drywell sump level monitoring, and drywell air cooler condensate flow rate monitoring equipment can detect within a reasonable time period. Violation of this LCO could result in continued degradation of the RCPB.

c. Total LEAKAGE

The total LEAKAGE limit is based on a reasonable minimum detectable amount. The limit also accounts for LEAKAGE from known sources (identified LEAKAGE). Violation of this LCO indicates an unexpected amount of LEAKAGE and, therefore, could indicate new or additional degradation in an RCPB component or system.

APPLICABILITY

In MODES 1, 2, 3, and 4, the RCS operational LEAKAGE LCO applies because the potential for RCPB LEAKAGE is greatest when the reactor is pressurized.

In MODES 5 and 6, compliance with the RCS operational LEAKAGE limits is not required because the reactor is not pressurized and stresses in the RCPB materials and potential for LEAKAGE are reduced.

ACTIONS

A.1

With RCS LEAKAGE greater than the limits for reasons other than pressure boundary LEAKAGE, actions must be taken to reduce LEAKAGE to within limits. Because the LEAKAGE limits are conservatively below the LEAKAGE that would constitute a critical crack size, 4 hours are allowed to verify the source and reduce the LEAKAGE rates before the reactor must be shut down. A change in unidentified LEAKAGE that has been identified and quantified may be reclassified and considered as identified LEAKAGE. However, the total LEAKAGE limit would remain unchanged. The 4-hour Completion Time is needed to properly verify the source and reduce the LEAKAGE before the reactor must be shut down.

BASES

ACTIONS (continued)

B.1 and B.2

If any Required Action and associated Completion Time of Condition A is not met or if pressure boundary LEAKAGE exists, 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 12 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 3.4.2.1

The RCS LEAKAGE is monitored by a variety of instruments designed to provide alarms when LEAKAGE is indicated and to quantify the various types of LEAKAGE. Leakage detection instrumentation is discussed in more detail in the Bases for LCO 3.3.4.1, “RCS Leakage Detection Instrumentation.” Sump level and flow rate are typically monitored to determine actual LEAKAGE rates. However, any method may be used to quantify LEAKAGE within the guidelines of Reference 5. In conjunction with alarms and other administrative controls, a 12-hour Frequency for this Surveillance is appropriate for identifying changes in LEAKAGE and for tracking required trends (Ref. 6).

REFERENCES

1. 10 CFR 50.2.
2. 10 CFR 50.55a(c).
3. 10 CFR 50, Appendix A, Section V, GDC 55.
4. 10 CFR 50, Appendix A, Section IV, GDC 30.
5. Regulatory Guide 1.45.
6. Generic Letter 88-01, Supplement 1.

B 3.4 REACTOR COOLANT SYSTEM (RCS)

B 3.4.3 RCS Specific Activity

BASES

BACKGROUND

During circulation, the reactor coolant acquires radioactive materials due to release of fission-products from fuel leaks into the coolant and activation of corrosion products in the reactor coolant. These radioactive materials in the coolant can plate out in the RCS, and, at times, an accumulation will break away to spike the normal level of radioactivity. The release of coolant during an accident could send radioactive materials into the environment.

Limits on the maximum allowable level of radioactivity in the reactor coolant are established to ensure, in the event of a release of any radioactive material to the environment during an accident, radiation doses are maintained within the limits of 10 CFR 52.47(a)(2)(iv) (Ref. 1).

This LCO contains iodine specific activity limits. The iodine isotopic activities per gram of reactor coolant are expressed in terms of a DOSE EQUIVALENT I-131. The allowable levels are intended to limit the 2-hour radiation dose to an individual at the site boundary to within the 10 CFR 52.47(a)(2)(iv) limit.

APPLICABLE SAFETY ANALYSES

Analytical methods and assumptions involving radioactive material in the primary coolant are presented in Reference 2. The specific activity in the reactor coolant (the source term) is an initial condition for evaluation of the consequences of an accident due to a:

1. Main steam line break (MSLB) outside containment
2. Feedwater line break (FWLB) outside containment
3. Small line break outside containment, or
4. Reactor Water Cleanup / Shutdown Cooling (RWCU/SDC) System line break outside containment.

The RWCU/SDC System line break outside containment release is the bounding accident with respect to offsite doses (Ref. 2). The limits on the specific activity of the primary coolant ensure that the 2-hour Total Effective Dose Equivalent (TEDE) doses at the site boundary, resulting from an RWCU/SDC System line break outside containment during steady state operations, will not exceed the dose guidelines of Regulatory Guide 1.183 (Ref. 3).

BASES

APPLICABLE SAFETY ANALYSES (continued)

The limits on specific activity are values from a parametric evaluation of typical site locations. These limits are conservative because the evaluation considered more restrictive parameters than for a specific site, such as the location of the site boundary and the meteorological conditions of the site.

RCS specific activity satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

The specific iodine activity is limited to ≤ 7400 Bq/gm (0.2 μCi/gm) DOSE EQUIVALENT I-131. This limit ensures the source term assumed in the safety analysis is not exceeded, so any release of radioactivity to the environment during an RWCU/SDC System line break outside containment is less than the Regulatory Guide 1.183 limits.

APPLICABILITY

In MODE 1, and MODES 2, 3, and 4, limits on the primary coolant radioactivity are applicable because there is an escape path for release of radioactive material from the primary coolant to the environment in the event of line breaks outside of primary containment.

In MODES 5 and 6, no limits are required because the reactor is not pressurized and the potential for leakage is reduced.

ACTIONS

A.1 and A.2

When the reactor coolant specific activity exceeds the LCO DOSE EQUIVALENT I-131 limit, but is ≤ 148,000 Bq/gm (4.0 μCi/gm), samples must be analyzed for DOSE EQUIVALENT I-131 at least once every 4 hours. In addition, the specific activity must be restored to the LCO limit within 48 hours. The Completion Time of once every 4 hours is the time needed to take and analyze a sample. The 48-hour Completion Time to restore the activity level provides a reasonable time for temporary coolant activity increases (iodine spikes or crud bursts) to be cleaned up with the normal processing systems.

BASES

ACTIONS (continued)

B.1, B.2, and B.3

If the DOSE EQUIVALENT I-131 cannot be restored to ≤ 7400 Bq/gm (0.2 µCi/gm) within 48 hours, or if at any time it is > 148,000 Bq/gm (4.0 µCi/gm), it must be determined at least every 4 hours.

The plant must be brought to MODE 3 within 12 hours and to MODE 5 within 36 hours. These actions reduce the potential for leakage by reducing RCS pressure and core thermal energy. In MODE 5, the requirements of the LCO are no longer applicable.

The Completion Time of once every 4 hours is the time needed to take and analyze a sample. The allowed Completion Times for Required Actions B.2 and B.3 for bringing the plant to MODES 3 and 5 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 3.4.3.1

This Surveillance is performed to ensure iodine remains within limit during normal operation. The 7-day Frequency is adequate to trend changes in the iodine activity level.

This SR is modified by a Note that requires this Surveillance to be performed only in MODE 1 because the level of fission products generated in other MODES is much less.

REFERENCES

1. 10 CFR 52.47(a)(2)(iv).
2. Section 15.4.
3. Regulatory Guide 1.183, “Alternative Radiological Source Terms for Evaluating Design Basis Accidents at Nuclear Power Plants,” July 2000.

B 3.4 REACTOR COOLANT SYSTEM (RCS)

B 3.4.4 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.

COL 16.0-1-A 3.4.4-1

[The PTLR] contains P/T limit curves for heatup, cooldown, and inservice leak and hydrostatic testing, and data for the maximum rate of change of reactor coolant temperature. The heatup curve provides limits for both heatup and criticality.

Each P/T limit curve defines an acceptable region for normal operation. The usual use of the curves is operational guidance during heatup or cooldown maneuvering, when pressure and temperature indications are monitored and compared to the applicable curve to determine that operation is within the allowable region.

The LCO establishes operating limits that provide a margin to brittle failure of the reactor vessel and piping of the reactor coolant pressure boundary (RCPB). The vessel is the component of most concern in regard to brittle failure. Therefore, the LCO limits apply mainly to the vessel.

10 CFR 50, Appendix G (Ref. 1), requires the establishment of P/T limits for material fracture toughness requirements of the RCPB materials. Reference 1 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 III, Appendix G (Ref. 2).

The actual shift in the Reference Temperature, Nil-Ductility Transition (RT_{NDT}) of the vessel material will be established periodically by removing and evaluating the irradiated reactor vessel material specimens, in accordance with ASTM E 185 (Ref. 3) and 10 CFR 50, Appendix H (Ref. 4). The operating P/T limit curves will be adjusted as necessary, based on the evaluation findings and the recommendations of Reference 5.

BASES

BACKGROUND (continued)

The P/T limit curves are composite curves established by superimposing limits derived from stress analyses of those portions of the reactor vessel and head that are the most restrictive. At any specific pressure, temperature, and temperature rate of change, one location within the reactor vessel will dictate the most restrictive limit. Across the span of the P/T limit curves, different locations are more restrictive, and, thus, the curves are composites of the most restrictive regions.

The criticality limits include the Reference 1 requirement that they be at least 22°C (40°F) above the heatup curve or the cooldown curve and not lower than the minimum permissible temperature for the inservice leak and hydrostatic testing.

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.

APPLICABLE SAFETY ANALYSES

The P/T limits are not derived from Design Basis Accident (DBA) analyses. They are prescribed during normal operation to avoid encountering pressure, temperature, and temperature rate-of-change conditions that might cause undetected flaws to propagate and cause non-ductile failure of the RCPB, a condition that is unanalyzed. Reference 6 establishes the methodology for determining the P/T limits. Because the P/T limits are not derived from any DBA, there are no acceptance limits related to the P/T limits. Rather, the P/T limits are acceptance limits themselves because they preclude operation in an unanalyzed condition.

RCS P/T limits satisfy Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

The elements of this LCO are:

COL 16.0-1-A 3.4.4-1

a. RCS pressure, temperature, and heatup or cooldown rate are within the limits specified in [the PTLR];

COL 16.0-1-A 3.4.4-1

b. RCS pressure and temperature are within the criticality limits specified in [the PTLR], prior to achieving criticality; and

BASES

LCO (continued)

COL 16.0-1-A
3.4.4-1

c. Reactor vessel flange and the head flange temperatures are within the limits of [the PTLR] when tensioning reactor vessel head bolting studs.

These limits define allowable operating regions and permit a large number of operating cycles while also providing a wide margin to non-ductile failure.

The temperature rate-of-change limits control the thermal gradient through the vessel wall and are used as inputs for calculating the heatup, cooldown, and inservice leak and hydrostatic 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 limits places the reactor vessel outside of the bounds of the stress analyses and can increase stresses in other RCS components. The consequences depend on several factors, as follow:

a. The severity of the departure from the allowable operating pressure temperature regime or the severity of the rate-of-change of temperature;

b. The length of time the limits were violated (longer violations allow the temperature gradient in the thick vessel walls to become more pronounced); and

c. The existence, size, and orientation of flaws in the vessel material.

APPLICABILITY

The potential for violating a P/T limit exists at all times. For example, P/T limit violations could result from ambient temperature conditions that result in the reactor vessel metal temperature being less than the minimum allowed temperature for boltup. Therefore, this LCO is applicable even when fuel is not loaded in the core.

BASES

ACTIONS

A.1 and A.2

Operation outside the P/T limits while in MODES 1, 2, 3,or 4 must be corrected so that the RCPB is returned to a condition that has been verified by stress analyses.

The 30-minute Completion Time reflects the urgency of restoring the parameters to within the analyzed range. Most violations will not be severe, and the activity can be accomplished in this time in a controlled manner.

Besides restoring operation 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 if continued operation is desired. Several methods may be used, including comparison with pre-analyzed transients in the stress analyses, new analyses, or inspection of the components.

The 72-hour Completion Time is reasonable to accomplish the evaluation. The evaluation for a mild violation is possible within this time, but more severe violations may require special, event-specific stress analyses or inspections. A favorable evaluation must be completed if continued operation beyond the 72 hours is desired.

Condition A is modified by a Note requiring Required Action A.2 be completed whenever the Condition is entered. The Note emphasizes the need to perform the evaluation of the effects of the excursion outside the allowable limits. Restoration alone per Required Action A.1 is insufficient because higher than analyzed stresses may have occurred and may have affected the RCPB integrity.

B.1 and B.2

If a Required Action and associated Completion Time of Condition A are not met, the plant must be brought to a lower MODE because either the RCS remained in an unacceptable P/T region for an extended period of increased stress, or a sufficiently severe event caused entry into an unacceptable region. Either possibility indicates a need for more careful examination of the event, best accomplished with the RCS at reduced pressure and temperature. With the reduced pressure and temperature conditions, the possibility of propagation of undetected flaws is decreased.

Pressure and temperature are reduced by bringing the plant to at least MODE 3 within 12 hours and to MODE 5 within 36 hours. The allowed

BASES

ACTIONS (continued)

Completion Times are reasonable based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

C.1 and C.2

Operation outside the P/T limits in other than MODES 1, 2, 3, and 4 (including defueled conditions) must be corrected so that the RCPB is returned to a condition that has been verified by stress analyses. The Required Action must be initiated without delay and continued until the limits are restored.

Besides restoring the P/T limit parameters to within limits, an evaluation is required to determine if RCS operation is allowed. This evaluation must verify that the RCPB integrity is acceptable and must be completed before approaching criticality or heating up to > 93.3°C (200°F). Several methods may be used, including comparison with pre-analyzed transients, new analyses, or inspection of the components.

Condition C is modified by a Note requiring Required Action C.2 be completed whenever the Condition is entered. The Note emphasizes the need to perform the evaluation of the effects of the excursion outside the allowable limits. Restoration alone per Required Action C.1 is insufficient because higher than analyzed stresses may have occurred and may have affected the RCPB integrity.

SURVEILLANCE REQUIREMENTS

SR 3.4.4.1

Verification that operation is within limits is required every 30 minutes when RCS pressure and temperature conditions are undergoing planned changes. This Frequency is considered reasonable in view of the control room indication available to monitor RCS status. Also, since temperature rate-of-change limits are specified in hourly increments, 30 minutes permits assessment and correction of minor deviations.

Surveillance for heatup, cooldown, or inservice leak and hydrostatic testing may be discontinued when the definition given in the relevant plant procedure for ending the activity is satisfied.

This SR has been modified by a Note that requires this Surveillance to be performed only during system heatup, and cooldown operations and inservice leak and hydrostatic testing.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.4.4.2

A separate limit is used when the reactor is approaching criticality. Consequently, the RCS pressure and temperature must be verified within the appropriate limits before withdrawing control rods that will make the reactor critical.

Performing the Surveillance within 15 minutes before control rod withdrawal for the purpose of achieving criticality provides adequate assurance that the limits will not be exceeded between the time of the Surveillance and the time of the control rod withdrawal.

SR 3.4.4.3, SR 3.4.4.4, and SR 3.4.4.5

Limits on the reactor vessel flange and head flange temperatures are generally bounded by the other P/T limits during system heatup and cooldown. However, operations approaching MODE 5 and MODE 6 and in MODE 5 with RCS temperature less than or equal to certain specified values require assurance that these temperatures meet the LCO limits.

COL 16.0-1-A 3.4.4-1

COL 16.0-1-A 3.4.4-2

The flange temperatures must be verified to be above the limits 30 minutes before and while tensioning the vessel head bolting studs to ensure that once the head is tensioned the limits are satisfied. When in MODE 5 with RCS temperature ≤ [26.7°C (80°F)], 30-minute checks of the flange temperatures are required because of the reduced margin to the limits. When in MODE 5 with RCS temperature ≤ [37.8°C (100°F)], monitoring of the flange temperature is required every 12 hours to ensure the temperatures are within the limits specified in [the PTLR].

The 30-minute Frequency reflects the urgency of maintaining the temperatures within limits, and also limits the time that the temperature limits could be exceeded. The 12-hour Frequency is reasonable based on the rate of temperature change possible at these temperatures.

REFERENCES

1. 10 CFR 50, Appendix G.

2. ASME, Boiler and Pressure Vessel Code, Section III, Appendix G.

3. ASTM E 185-82.

4. 10 CFR 50, Appendix H.

BASES

REFERENCES (continued)

5. Regulatory Guide 1.99, Revision 2, May 1988.

COL 16.0-1-A 3.4.4-3 [6. P/T Limits Methodology Topical.]

B 3.4 REACTOR COOLANT SYSTEM (RCS)

B 3.4.5 Reactor Steam Dome Pressure

BASES

BACKGROUND	The reactor steam dome pressure is an assumed initial condition of Design Basis Accidents (DBAs) and is also an assumed value in the determination of compliance with reactor pressure vessel overpressure protection criteria.
APPLICABLE SAFETY ANALYSES	The reactor steam dome pressure of ≤ 7.17 MPaG (1040 psig) is an initial condition of the vessel overpressure protection analysis of Reference 1. This analysis assumes an initial maximum reactor steam dome pressure and evaluates the response of the pressure relief system, primarily the safety relief valves, during the limiting pressurization transient. The determination of compliance with the overpressure criteria is dependent on the initial reactor steam dome pressure; therefore, the limit on this pressure ensures that the assumptions of the overpressure protection analysis are conserved. Reference 1 also assumes an initial reactor steam dome pressure for the analysis of DBAs and transients used to determine the limits for fuel cladding integrity MCPR (see Bases for LCO 3.2.2, “MINIMUM CRITICAL POWER RATIO (MCPR)”). Reactor steam dome pressure satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).
LCO	The specified reactor steam dome pressure limit of ≤ 7.17 MPaG (1040 psig) ensures the plant is operated within the assumptions of the transient analyses. Operation above the limit may result in a transient response more severe than analyzed.
APPLICABILITY	In MODES 1 and 2, the reactor steam dome pressure is required to be less than or equal to the limit. In these MODES the reactor may be generating significant steam and the DBAs and transients are bounding. In MODES 3, 4, 5, and 6, the limit is not applicable because the reactor is shutdown. In these MODES, the reactor pressure is well below the required limit, and no anticipated events will challenge the overpressure limits.

BASES

ACTIONS

A.1

With the reactor steam dome pressure greater than the limit, prompt action should be taken to reduce pressure to below the limit and return the reactor to operation within the bounds of the analyses. The 15-minute Completion Time is reasonable considering the importance of maintaining the pressure within limits. This Completion Time also ensures that the probability of an accident while pressure is greater than the limit is minimal. If the operator is unable to restore the reactor steam dome pressure to below the limit, then the reactor should be brought to MODE 3 to be within the assumptions of the transient analyses.

B.1

If the reactor steam dome pressure cannot be restored to within the limit 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 12 hours. The allowed Completion Time of 12 hours is reasonable, based on operating experience, to reach MODE 3 from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.4.5.1

Verification that reactor steam dome pressure is ≤ 7.17 MPaG (1040 psig) ensures that the initial conditions of the DBAs and transients are met. Operating experience has shown the 12-hour Frequency to be sufficient for identifying trends and verifying operation within safety analyses assumptions.

REFERENCES

1. Chapter 15.

B 3.5 EMERGENCY CORE COOLING SYSTEM (ECCS)

B 3.5.1 Automatic Depressurization System (ADS) - Operating

BASES

BACKGROUND

The ECCS function is provided by the combination of the Gravity-Driven Cooling System (GDCS), the Automatic Depressurization System (ADS), the Standby Liquid Control (SLC) System, and the Isolation Condenser System (ICS). The ECCS is designed to flood the core during a loss-of-coolant accident (LOCA) to provide required core cooling. By providing core cooling following a LOCA, the ECCS, in conjunction with the containment, limits the release of radioactive materials to the environment following a LOCA.

The ADS (Ref. 1) is an integral part of the ECCS because GDCS flow to the RPV requires the RPV to be close to containment pressure. Therefore, the ADS is designed to depressurize the RPV following indication of a LOCA. The ADS consists of eight squib-actuated depressurization valves (DPVs) and the ten Safety Relief valves (SRVs) that have been configured to function as ADS valves. The ten dual function SRVs are pneumatically actuated when functioning as ADS valves using energy stored in nitrogen accumulators.

Each of the eight DPVs is equipped with four squib initiators. A signal to any of the four squib initiators will actuate the DPV. Each of the ten SRVs is equipped with four actuation solenoids (i.e., initiators). A signal to any of the four solenoids will actuate the SRV. Three of the four initiators on each valve are actuated by the Safety System Logic and Control/Engineered Safety Features (SSLC/ESF) System described in the Bases for LCO 3.3.5.1, "Emergency Core Cooling System (ECCS) Instrumentation," and LCO 3.3.5.2, "Emergency Core Cooling System (ECCS) Actuation." The fourth initiator is actuated by the Diverse Protection System (DPS), which is designed to mitigate digital protection system common mode failures.

Power to each of the three safety-related initiators on each ECCS valve is supplied from a different division of the DC and Uninterruptible AC Electrical Power Distribution. As such, at least two of the three safety-related initiators in each ECCS valve will be associated with DC and Uninterruptible AC Electrical Power Distribution Divisions required by LCO 3.8.6, "Distribution Systems - Operating."

BASES

BACKGROUND (continued)

Actuation signals and logic for ADS initiation are described in the Bases of LCO 3.3.5.1. ADS initiation is sequenced beginning with the opening of five SRVs that reduce reactor pressure. The remaining five SRVs open after a short time delay. After another short time delay, the DPVs are staggered opened beginning with a group of three DPVs, followed by consecutive groups of two, two and one DPV with a short time delay between each group. This sequential operation facilitates rapid depressurization while minimizing the amount of water lost because of level swell in the reactor that occurs when pressure is rapidly reduced.

The ADS is designed to ensure that no single active component failure will cause inadvertent initiation of ADS or prevent automatic initiation and successful operation of the minimum required ECCS subsystems when any three of the four divisions of DC and Uninterruptible AC Electrical Power Distribution and the associated instrumentation divisions are OPERABLE.

APPLICABLE SAFETY ANALYSES

ADS performance is evaluated for the entire spectrum of break sizes for postulated LOCAs. The accidents for which ADS operation is required are presented in Reference 2. The required ECCS analyses and assumptions and the results of these analyses are described in References 1 and 2. This LCO ensures that the following acceptance criteria for the ECCS, established by 10 CFR 50.46 (Ref. 3), will be met following a LOCA assuming the worst-case single active component failure in the ECCS:

a. Maximum fuel element cladding temperature is ≤ 1204°C (2200°F).

b. Maximum cladding oxidation is ≤ 0.17 times the total cladding thickness before oxidation.

c. Maximum hydrogen generation from zirconium-water reaction is ≤ 0.01 times the hypothetical amount that would be generated if all of the metal in the cladding surrounding the fuel, excluding the cladding surrounding the plenum volume, were to react.

d. The core is maintained in a coolable geometry.

e. Adequate long-term cooling capability is maintained.

BASES

APPLICABLE SAFETY ANALYSES (continued)

Each break location is analyzed assuming each potential failure to determine the most limiting single failure for the LOCA event to ensure that the remaining OPERABLE ECCS subsystems provide the capability to adequately cool the core and prevent excessive fuel damage. The limiting failures are discussed in Reference 1.

For ADS to support GDCS injection following a small break LOCA, the analysis in Reference 1 assumes the single failure of either one DPV or one SRV. At least three Isolation Condenser loops, two SLC trains, and the minimum required complement of GDCS injection and equalizing lines are assumed to be available during the LOCA.

The ADS satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

This LCO for ADS requires the OPERABILITY of the following:

a. The ADS function of ten SRVs; and

b. Eight DPVs.

OPERABILITY of each DPV and SRV requires OPERABILITY of the DPS initiator and two safety-related initiators associated with DC and Uninterruptible AC Electrical Power Distribution Divisions required by LCO 3.8.6.

OPERABILITY of the ADS function of the SRVs also requires that SRV nitrogen accumulator pressure be within the limit specified by SR 3.5.1.1.

APPLICABILITY

ADS is required to be OPERABLE during MODES 1, 2, 3, and 4 when there is considerable energy in the reactor core and core cooling may be required to prevent fuel damage following a LOCA. ADS requirements for MODES 5 and 6 are determined by the requirements of the GDCS system, which is being supported.

BASES

ACTIONS

A.1

This Condition applies when one ADS valve has an inoperable DPS initiator. In this Condition, required safety-related initiators will actuate the minimum number of ADS valves assumed in the design basis LOCA analysis in Reference 1 concurrent with any additional single failure, including digital protection system common mode failures.

In this Condition, the inoperable DPS initiator must be restored to OPERABLE status the next time the plant is placed in MODE 5 (i.e., prior to entering MODE 2 or MODE 4 from MODE 5). This Completion Time is acceptable because the remaining DPS initiator and the required safety-related initiators will actuate the minimum number of ADS valves required to respond to the design basis LOCA concurrent with any additional single failure.

B.1

This Condition applies when two or more DPS initiators are inoperable. In this Condition, required safety-related initiators will actuate the minimum number of ADS valves assumed in the design basis LOCA analysis in Reference 1 concurrent with any additional single failure. However, design features intended to mitigate the possibility of digital protection system common mode failures are not available.

In this Condition, all but one DPS initiator must be restored to OPERABLE status within 30 days. This Completion Time is acceptable because the required safety-related initiators will actuate the minimum number of ADS valves required to respond to the design basis LOCA concurrent with any additional single failure.

C.1

This Condition applies when one ADS valve (i.e., either one DPV or one SRV) is inoperable for reasons other than Condition A. In this Condition, failure of a second ADS valve could result in less than the minimum required ADS capacity during a design basis LOCA.

In this Condition, the inoperable ADS valve must be restored to OPERABLE status within 14 days. This Completion Time is acceptable based on engineering judgment considering the low probability of a failure of an additional DPV or SRV concurrent with a design basis LOCA during this period.

BASES

ACTIONS (continued)

D.1 and D.2

This Condition applies when two or more ADS valves (i.e., any combination of DPVs or SRVs) are inoperable for reasons other than Conditions A or B. This Condition also applies when the Required Actions and Completion Times of Conditions A, B, or C are not met. In this Condition, 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 12 hours and to MODE 5 within 36 hours. The allowed Completion Times are reasonable, based on plant design, to reach required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.5.1.1

This SR requires periodic verification that the supply pressure to SRV accumulators (i.e., High Pressure Nitrogen Supply System (HPNSS)) is greater than or equal to the specified limit. An accumulator on each SRV provides pneumatic pressure for ADS valve actuation. The SRV accumulator capacity is sufficient for one actuation at drywell design pressure following a failure of the gas supply to the accumulator.

The 31-day Frequency is acceptable because HPNSS low pressure alarms provide prompt notification of an abnormal pressure in the HPNSS.

SR 3.5.1.2

This SR requires verification every 31 days of the continuity of the DPS initiator and two safety-related initiators associated with DC and Uninterruptible AC Electrical Power Distribution Divisions required by LCO 3.8.6, “Distribution Systems - Operating.”

The 31-day Frequency is acceptable because either of the two safety-related initiators in each valve is capable of actuating the associated ADS valve. Additionally, an alarm will provide prompt notification of loss of circuit continuity for the required initiators in each ADS valve.

BASES

SURVEILLANCE REQUIREMENTS (continued)

This SR is modified by a Note that continuity is not required to be met for one required initiator intermittently disabled under administrative controls. This allows the continuity monitor to be tested and allows surveillance and maintenance with the assurance that the valve will not be opened inadvertently. The operation of the disable/test switch in either division does not disable the ADS valve because the valve will still be opened by the initiator in the other division.

SR 3.5.1.3

This SR requires periodic verification that the ADS function of each SRV actuates on an actual or simulated automatic initiation signal. The ADS function of each SRV is required to actuate automatically to perform its design function. The LOGIC SYSTEM FUNCTIONAL TEST in LCO 3.3.5.2 and LCO 3.3.8.1 overlap this SR to provide complete testing of the assumed safety function.

This SR is modified by a Note that excludes SRV valve actuation as a requirement for this SR to be met. This is acceptable because SRVs are tested in accordance with the Inservice Test Program.

The 24-month Frequency for performing this SR 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 SR were performed with the reactor at power. From past operating experience, it is believed that these components will pass the SR when performed once per the 24-month refueling interval.

SR 3.5.1.4

This SR requires periodic verification that the ADS function of each DPV actuates on an actual or simulated automatic initiation signal. The ADS function of each DPV is required to actuate automatically to perform their design functions. The LOGIC SYSTEM FUNCTIONAL TEST in LCO 3.3.5.2 overlaps this SR to provide complete testing of the assumed safety function.

This SR is modified by a Note that excludes squib valve actuation as a requirement for this SR to be met. This is acceptable because the design of the squib-actuated valve was selected for this application because of its very high reliability. The OPERABILITY of squib-actuated valves is verified by continuity tests in SR 3.5.1.2 and the Inservice Test Program for squib-actuated valves.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The 24-month Frequency for performing this SR is based on the need to perform this SR under the conditions that apply during a plant outage and the potential for an unplanned transient if the SR were performed with the reactor at power. Operating experience has shown that these components usually pass the SR when performed once per the 24-month refueling interval.

REFERENCES

1. Chapter 6.
2. Chapter 15.
3. 10 CFR 50.46.

B 3.5 EMERGENCY CORE COOLING SYSTEM (ECCS)

B 3.5.2 Gravity-Driven Cooling System (GDCS) - Operating

BASES

BACKGROUND

The ECCS function is provided by the combination of the Gravity-Driven Cooling System (GDCS), the Automatic Depressurization System (ADS), the Standby Liquid Control (SLC) System, and the Isolation Condenser System (ICS). The ECCS is designed to flood the core during a loss-of-coolant accident (LOCA) to provide required core cooling. By providing core cooling following a LOCA, the ECCS, in conjunction with the containment, limits the release of radioactive materials to the environment following a LOCA.

The GDCS (Ref. 1) is divided into three subsystems: the GDCS short-term cooling (injection subsystem); the GDCS long-term cooling (equalizing subsystem); and, the GDCS deluge subsystem. Three GDCS pools, located above the wetwell, at an elevation above the reactor core, contain the water that supports all four GDCS trains for the injection and deluge subsystems.

The GDCS injection subsystem is capable of refilling the RPV following a LOCA after the RPV is depressurized by the ADS. Each of the four injection trains connects to the associated GDCS pool through a single pipe that includes a block valve at the pool. Each of the four injection trains then divides into two branch lines after entering the drywell. The resulting eight injection branch lines each include a check valve, squib-actuated injection valve, and a block valve near the RPV. Each injection branch line provides coolant to the annulus region of the reactor through an RPV nozzle located above the top of active fuel (TAF).

The GDCS equalizing subsystem provides long term post-LOCA water makeup by connecting the annulus region of the reactor to the suppression pool. Each of the four equalizing trains includes a block valve at the suppression pool, a check valve, a squib-actuated equalizing valve, and a block valve at the RPV. The suppression pool is located in the containment with a normal level above the top of the core.

The GDCS deluge subsystem is used to dump water from the GDCS pools to the lower drywell in the event of a severe accident. The deluge subsystem is designed to respond to a severe accident and is not required in any accident analysis in Reference 1. Therefore, OPERABILITY of the GDCS deluge subsystems is not required by Technical Specifications and is addressed in licensee controlled documents.

BASES

BACKGROUND (continued)

Each of the eight GDCS injection subsystem squib valves is equipped with four squib initiators. A signal to any of the four initiators will actuate the valve. Three of the four initiators on each valve are actuated by the Safety System Logic and Control/Engineered Safety Features (SSLC/ESF) System described in the Bases for LCO 3.3.5.1, "Emergency Core Cooling System (ECCS) Instrumentation" and LCO 3.3.5.2, "Emergency Core Cooling System (ECCS) Actuation." The fourth initiator is actuated by the Diverse Protection System (DPS), which is designed to mitigate digital protection system common mode failures.

Each of the four GDCS equalizing train squib valves is equipped with four squib initiators. A signal to any of the four initiators will actuate the valve. Three initiators on each valve are actuated by the SSLC/ESF described in the Bases for LCO 3.3.5.1 and LCO 3.3.5.2. The fourth initiator is actuated by the DPS. The equalizing trains are needed for the long term cooling only and are not automatically actuated by the DPS. The DPS initiator is provided only for manual initiation of the equalizing train.

Power to each of the three safety-related initiators on each ECCS valve is supplied from a different division of the DC and Uninterruptible AC Electrical Power Distribution. As such, at least two of the three initiators in each ECCS valve will be associated with divisions required by LCO 3.8.6, "Distribution Systems - Operating."

The GDCS is designed to ensure that no single active component failure will cause inadvertent initiation of GDCS or prevent automatic initiation and successful operation of the minimum required ECCS subsystems when any three of the four divisions of DC and Uninterruptible AC Electrical Power Distribution and the associated instrumentation divisions are OPERABLE.

Although the nominal and bounding containment performance analyses are performed at an initial condition of 46.1ºC (115ºF) for the GDCS pool water temperature, additional analyses assuming GDCS pool water temperature as high as 65.5ºC (150ºF) were performed. These analyses demonstrate the relative insensitivity of the calculated peak containment pressure and temperature and reactor pressure vessel long-term water level after a DBA for increased GDCS pool water initial temperature. Therefore, monitoring of the GDCS pool temperature is not required.

BASES

APPLICABLE SAFETY ANALYSES

GDCS performance is evaluated for the entire spectrum of break sizes for postulated LOCAs. The accidents for which GDCS operation is required are presented in Reference 1. The required ECCS analyses and assumptions and the results of these analyses are described in References 1 and 2.

This LCO ensures that the following acceptance criteria for the ECCS, established by 10 CFR 50.46 (Ref. 3), will be met following a LOCA assuming the worst-case single active component failure in the ECCS:

a. Maximum fuel element cladding temperature is ≤ 1204°C (2200°F).

b. Maximum cladding oxidation is ≤ 0.17 times the total cladding thickness before oxidation.

c. Maximum hydrogen generation from zirconium-water reaction is ≤ 0.01 times the hypothetical amount that would be generated if all of the metal in the cladding surrounding the fuel, excluding the cladding surrounding the plenum volume, were to react.

d. The core is maintained in a coolable geometry.

e. Adequate long-term cooling capability is maintained.

Each break location is analyzed assuming each potential failure to determine the most limiting single failure for the LOCA event to ensure that the remaining OPERABLE ECCS subsystems provide the capability to adequately cool the core and prevent excessive fuel damage. Both the injection and equalizing subsystems are designed to ensure that adequate reactor vessel inventory is provided assuming the initiating event is a LOCA in one train and there is a failure of one squib valve to actuate in a second train.

The analysis described in Reference 1 determined that the GDCS injection subsystem is capable of providing the minimum required core cooling following a LOCA initiated by a break in an injection branch line with a concurrent failure of any other injection branch line. The break in an injection branch line is assumed to disable the injection capability of both injection branch lines in that injection train. Additionally, this analysis determined that the GDCS equalizing trains are capable of providing the minimum required long-term core cooling following a LOCA initiated by a break in an equalizing train with a concurrent failure of any other equalizing train.

BASES

APPLICABLE SAFETY ANALYSES (continued)

The GDCS satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

This LCO requires the OPERABILITY of the following:

a. Eight branch lines of the injection subsystem (i.e., all four injection trains); and

b. Four trains of the equalizing subsystem.

OPERABILITY of each squib-actuated GDCS valve in the injection subsystem and equalizing subsystem requires OPERABILITY of the DPS initiator and two safety-related initiators associated with DC and Uninterruptible AC Electrical Power Distribution Divisions required by LCO 3.8.6.

OPERABILITY of each GDCS branch line requires that water level in the associated GDCS pool be within the limit specified by SR 3.5.2.1. Additionally, all GDCS RPV block valves, GDCS pool block valves, and suppression pool block valves must be locked open.

APPLICABILITY

GDCS subsystems are required to be OPERABLE during MODES 1, 2, 3, and 4 when there is considerable energy in the reactor core and core cooling may be required to prevent fuel damage following a LOCA. GDCS requirements for MODES 5 and 6 are specified in LCO 3.5.3, “Gravity-Driven Cooling System (GDCS) - Shutdown.”

ACTIONS

A.1

This Condition applies when one or more GDCS subsystems have one inoperable DPS initiator. In this Condition, required safety-related initiators will actuate the minimum number of GDCS valves assumed in the design basis LOCA analysis in Reference 1 concurrent with any additional single failure, including digital protection system common mode failures.

BASES

ACTIONS (continued)

In this Condition, the inoperable DPS initiators must be restored to OPERABLE status the next time the plant is placed in MODE 5 (i.e., prior to entering MODE 2 or MODE 4 from MODE 5). This Completion Time is acceptable because the remaining DPS initiators and the required safety-related initiators will actuate the minimum number of GDCS valves required to respond to the design basis LOCA concurrent with any additional single failure.

B.1

This Condition applies when one or more GDCS subsystems have two or more inoperable DPS initiators. In this Condition, required safety-related initiators will actuate the minimum number of GDCS subsystem valves assumed in the design basis LOCA analysis in Reference 1 concurrent with any additional single failure. However, design features intended to mitigate the possibility of digital protection system common mode failures are not available.

In this Condition, all but one DPS initiator in each GDCS subsystem must be restored to OPERABLE status within 30 days. This Completion Time is acceptable because the required safety-related initiators will actuate the minimum number of GDCS subsystem valves required to respond to the design basis LOCA concurrent with any additional single failure.

C.1

This Condition applies when one GDCS injection subsystem branch line is inoperable for reasons other than Condition A or B. In this Condition, the minimum number of GDCS injection subsystem branch lines required for a design basis LOCA remain OPERABLE. However, failure of a second injection subsystem branch line could result in less than the minimum required GDCS injection capacity assumed in the design basis LOCA analysis in Reference 1.

In this Condition, the inoperable GDCS injection subsystem branch line must be restored to OPERABLE status within 14 days. This Completion Time is acceptable based on engineering judgment considering the low probability of a failure of an additional GDCS injection subsystem branch line concurrent with a design basis LOCA during this period.

BASES

ACTIONS (continued)

D.1

This Condition applies when one GDCS equalizing train is inoperable for reasons other than Condition A or B. In this Condition, the minimum number of GDCS equalizing trains required for a design basis LOCA remain OPERABLE. However, failure of a second equalizing train could result in less than the minimum required GDCS injection capacity assumed in the design basis LOCA analysis in Reference 1.

In this Condition, the inoperable GDCS equalizing train must be restored to OPERABLE status within 14 days. This Completion Time is acceptable based on engineering judgment considering the low probability of a failure of an additional GDCS equalizing train concurrent with a design basis LOCA during this period.

E.1 and E.2

This Condition applies when two or more injection branch lines or two or more equalizing trains are inoperable for reasons other than Condition A or B. In this Condition, the plant may not have sufficient GDCS capability to respond to a design basis LOCA. This Conditions also applies when Required Actions and Completion Time of Conditions A, B, C, or D are not met. In this Condition, 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 12 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 3.5.2.1

This SR requires verification every 12 hours that the water level in each of the GDCS pools is within the specified limit. The minimum specified level ensures there is a sufficient volume of water in the drywell to ensure the core remains covered following a severe LOCA and support decay heat removal without operator intervention for a minimum of 72 hours.

The 12-hour Frequency is acceptable because GDCS pool low level alarms will provide prompt notification of an abnormal level in any of the GDCS pools.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.5.2.2

This SR requires verification every 31 days of the continuity of the DPS initiator and two safety-related initiators associated with DC and Uninterruptible AC Electrical Power Distribution Divisions required by LCO 3.8.6 for each squib-actuated GDCS valve.

The 31-day Frequency is acceptable because either of the two safety-related initiators in each valve is capable of actuating the associated GDCS valve. Additionally, an alarm will provide prompt notification of loss of circuit continuity for the required initiators in each squib-actuated GDCS valve.

This SR is modified by a Note that continuity is not required to be met for one required initiator intermittently disabled under administrative controls. This allows the continuity monitor to be tested and allows surveillance and maintenance with the assurance that the valve will not be opened inadvertently. The operation of the disable/test switch in either division does not disable the GDCS valve because the valve will still be opened by the initiator in the other division.

SR 3.5.2.3

This SR requires verification every 24 months that each required GDCS valve actuates on an actual or simulated automatic initiation signal. The GDCS is required to actuate automatically to perform its design function. The LOGIC SYSTEM FUNCTIONAL TEST in LCO 3.3.5.2 and 3.3.8.1 overlap this SR to provide complete testing of the assumed safety function.

This SR is modified by a Note that excludes squib valve actuation as a requirement for this SR to be met. This is acceptable because the design of the squib-actuated valve was selected for this application because of its very high reliability. The OPERABILITY of squib-actuated valves is verified by continuity tests and the Inservice Test Program for squib-actuated valves.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The 24-month Frequency for performing this SR is based on the need to perform this SR under the conditions that apply during a plant outage and the potential for an unplanned transient if the SR were performed with the reactor at power. Operating experience has shown that these components usually pass the SR when performed once per the 24-month refueling interval.

SR 3.5.2.4 and SR 3.5.2.5

SR 3.5.2.4 requires verification every 24 months on a STAGGERED TEST BASIS that the flow path for each pair of GDCS injection branch lines, from the GDCS pool to the associated squib valve and the associated RPV injection nozzle, is not obstructed. SR 3.5.2.5 requires verification every 24 months on a STAGGERED TEST BASIS that the flow path for each GDCS equalizing line, from the suppression pool to the associated squib valve and the associated RPV injection nozzle, is not obstructed. Verification that the GDCS lines and RPV nozzles are not obstructed can be performed using the GDCS line test connections and any combination of flow tests, flushing, visual inspection, or boroscopic inspection.

These SRs are modified by a Note that excludes squib valve actuation as a requirement for the SR to be met. This is acceptable because test connections allow access to both sides of the squib-actuated valves, allowing verification that the flow path is free of obstructions without actuating the squib valve.

The Frequency for performing these SRs is based on engineering judgment. This Frequency is acceptable because cleanliness controls provide a high degree of assurance that foreign material that could obstruct the GDCS lines will not be introduced into the GDCS pools, the suppression pool, or reactor vessel.

REFERENCES

1. Chapter 6.
2. Chapter 15.
3. 10 CFR 50.46.

B 3.5 EMERGENCY CORE COOLING SYSTEMS (ECCS)

B 3.5.3 GDCS - Shutdown

BASES

BACKGROUND

A description of the ADS is provided in the Bases for LCO 3.5.1, "Automatic Depressurization System (ADS) - Operating." A description of the GDCS is provided in the Bases for LCO 3.5.2, "Gravity-Driven Cooling System (GDCS) - Operating."

In MODES 5 and 6, GDCS is used to provide additional water inventory inside the containment to respond to a loss of decay heat removal capability or a loss of reactor coolant inventory. Loss of decay heat removal capability could result from the unavailability of both Reactor Water Cleanup/Shutdown Cooling loops, loss of reactor component cooling water or plant service water systems, or loss of preferred power. Loss of reactor coolant inventory could result from pipe breaks in the RCS associated with maintenance or refueling, misalignment of systems connected to the RCS, or leakage during replacement of control rod drive assemblies.

GDCS pools with a minimum combined volume within the limit specified and the suppression pool provide additional water inventory to support decay heat removal for an extended period and makeup to respond to a loss of reactor coolant inventory.

ADS supports the GDCS function by providing a vent path that is adequate to maintain the RPV close to containment pressure following loss of decay heat removal capability. The number of ADS valves required to support GDCS is a function of core decay heat load.

APPLICABLE SAFETY ANALYSES

Three GDCS pools and the suppression pool provide sufficient inventory when in MODES 5 and 6 to respond to a loss of non-safety-related decay heat removal capability for 72 hours without reliance on the Isolation Condenser System (Ref. 2). Three GDCS pools and the suppression pool also provide additional water inventory inside the containment on a loss of reactor coolant inventory (Ref. 1). Three injection subsystem branch lines (i.e. one from each GDCS pool) and one equalizing train are required to supply the required makeup. ADS capacity equivalent to six depressurization valves (DPVs), which is

BASES

APPLICABLE SAFETY ANALYSES (continued)

sufficient to maintain the RPV close to containment pressure following a LOCA or loss of decay heat removal capability is required to support GDCS injection.

The GDCS satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

This LCO requires two injection subsystem branch lines associated with each of the three GDCS pools (i.e., six injection subsystem branch lines) and two equalizing subsystem trains. Additionally, to support OPERABILITY of the required GDCS subsystems, OPERABILITY of ADS valves (i.e., DPVs or SRVs or a combination of each) with relief capacity equivalent to six DPVs is required. These requirements ensure that the water inventory in three GDCS pools and the suppression pool will be injected in the event of any single failure.

OPERABILITY of each required squib-actuated GDCS valve and each required ADS valve requires OPERABILITY of two safety-related initiators associated with DC and Uninterruptible AC Electrical Power Distribution Divisions required by LCO 3.8.7, "Distribution Systems - Shutdown."

APPLICABILITY

Two injection subsystem branch lines associated with each of the three GDCS pools, two equalizing subsystem trains, and ADS valves with relief capacity equivalent to six DPVs are required to be OPERABLE in MODES 5 and 6 to assure adequate coolant inventory and sufficient heat removal capability for the irradiated fuel in the core in response to a loss of decay heat removal capability, a LOCA, or an inadvertent draindown of the RPV. These requirements are not applicable when the buffer pool gate is removed and water level is above the specified level over the top of the reactor pressure vessel flange because of the additional inventory available when in this configuration.

BASES

ACTIONS

A.1

This Condition applies when one required GDCS injection branch line, one required GDCS equalizing train, or one required ADS valve is inoperable. In this Condition, the remaining OPERABLE branch lines, equalizing trains, and ADS valves provide sufficient RPV flooding capability to recover from a loss of decay heat removal capability, LOCA, or inadvertent vessel draindown. However, overall reliability is reduced.

Therefore, the inoperable branch line, equalizing train, and ADS valve must be restored to OPERABLE within 14 days. The Completion Time is based on engineering judgment considering the need for prompt action to establish an alternate method to supply RPV inventory makeup or the need for timely restoration of vent capacity sufficient to allow GDCS injection.

B.1

This Condition applies when two or more required injection subsystem branch lines are inoperable. In this Condition, water in one or more GDCS pools may not be available to respond to a loss of decay heat removal capability, LOCA, or inadvertent vessel draindown.

Required Action B.1 requires establishing at least two methods of injecting a combined water volume greater than or equal to the required GDCS pool volumes (1636 m^3 (57,775 ft^3)). Alternate sources and methods for water injection are identified in the plant's Abnormal and Emergency Operating Procedures. The method used to provide water for core flooding is based on plant conditions. The 4-hour Completion Time is based on engineering judgment considering the need for prompt action to establish an alternate method to supply RPV inventory makeup.

C.1

This Condition applies when two required equalizing subsystem trains are inoperable. In this Condition, water in the suppression pool may not be available to respond to a loss of decay heat removal capability, LOCA, or inadvertent vessel draindown.

BASES

ACTIONS (continued)

Required Action C.1 requires establishing at least two methods of injecting a combined water volume greater than or equal to the required suppression pool volume (799 m^3 (28,216 ft^3)). Alternate sources and methods for water injection are identified in the plant's Abnormal and Emergency Operating Procedures. The method used to provide water for core flooding is based on plant conditions. The 4-hour Completion Time is based on engineering judgment considering the need for prompt action to establish an alternate method to supply RPV inventory makeup.

D.1.1, D.1.2, D.2

This Condition applies when GDCS is inoperable due to two or more required ADS valves being inoperable. In this Condition, RPV venting capacity may not be sufficient to allow GDCS injection. Required Action D.1.1 requires that GDCS injection capability be restored within 4 hours by establishing RCS vent path(s) with relief capacity equivalent to the required ADS valves. Manually actuated ADS valves may be used to satisfy this requirement. RCS vent paths other than ADS valves may be used provided the vent path(s) establish an RCS vent equivalent to 6 DPVs and are maintained open. A combination of OPERABLE ADS valves and other open vent paths can satisfy this Required Action.

Alternately, Required Action D.1.2 requires establishing at least two methods of injecting a combined water volume greater than or equal to the required GDCS and suppression pool volumes ($\geq$ 2435 m^3 (85,991 ft^3)). Alternate sources and methods for water injection are identified in the plant's Abnormal and Emergency Operating Procedures. The method used to provide water for core flooding is based on plant conditions.

The Completion Times are based on engineering judgment considering the need for prompt action to establish an alternate method to supply RPV inventory makeup or the need for timely restoration of vent capacity sufficient to allow GDCS injection.

Required Action D.2 requires that LCO requirements be met within 72 hours. This Completion Time is based on engineering judgment considering the low probability of an event requiring GDCS injection when in this Condition.

ACTIONS (continued)

E.1 and E.2

If the LCO is not met for reasons other than Condition A, B, or C, action must be initiated to provide at least two methods of injecting the minimum specified volume of water into the RPV. In addition, LCO requirements must be met within 72 hours. This Completion Time is based on engineering judgment considering the low probability of an event requiring GDCS injection when in this Condition.

Alternate sources and methods for water injection are identified in the plant's Abnormal and Emergency Operating Procedures. The method used to provide water for core flooding is based on plant conditions.

F.1, F.2.1.and F.2.2

If Required Actions and associated Completion Times are not met, the water inventory available for injection may not be sufficient to respond to a loss of decay heat removal capability, LOCA, or inadvertent vessel draindown. Therefore, actions to suspend operations with a potential for draining the reactor vessel (OPDRVs) must be initiated immediately to minimize the probability of a vessel draindown. Actions must continue until OPDRVs are suspended. In addition, action must be initiated immediately to establish reactor building refueling and pool area HVAC subsystem (REPAVS) and contaminated area HVAC subsystem (CONAVS) area isolation boundary. This can be accomplished by isolating the REPAVS and CONAVS dampers or verifying the automatic isolation capability of the respective exhaust high radiation function. This action is needed to establish appropriate compensatory measures for a potential loss of decay heat removal as a result of an inadvertent draindown event. The Completion Times are based on engineering judgment considering the need for prompt action to mitigate the consequences of a potential loss of decay heat removal capability, LOCA, or inadvertent vessel draindown.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.5.3.1

This SR requires verification every 24 hours that the water level in each of the GDCS pools is within the specified limit. This SR ensures adequate inventory is maintained in the containment to respond to a loss of decay heat removal capability or a loss of reactor coolant due to a LOCA or inadvertent draining of the RPV.

The 24-hour Frequency is acceptable because highly reliable GDCS pool low level alarms will provide prompt notification of an abnormal level in any of the GDCS pools.

SR 3.5.3.2

This SR requires verification every 24 hours that suppression pool level is sufficient to support the required operation of the GDCS equalizing trains in response to loss of decay heat removal capability, LOCA, or inadvertent vessel draindown. The 24-hour Frequency is acceptable because suppression pool low level alarms will provide prompt notification of an abnormal level in the suppression pool.

SR 3.5.3.3

This SR requires periodic verification that the supply pressure to required SRV accumulators is greater than or equal to the specified limit. An accumulator on each SRV provides pneumatic pressure for ADS valve actuation. The SRV accumulator capacity is sufficient for one actuation following a failure of the gas supply to the accumulator.

SR 3.5.3.3 is modified by two Notes. Note 1 states that this SR is only required to be met in MODE 5 and in MODE 6 prior to removal of the reactor pressure vessel head. ADS is not required for GDCS injection following removal of the reactor pressure vessel head. Note 2 states that the SRV accumulator supply pressure is only required to be met for SRVs that are credited with meeting the necessary relief capacity equivalent to 6 depressurization valves (DPVs).

The 31-day Frequency is acceptable because low pressure alarms provide prompt notification of an abnormal pressure in the accumulator supply.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.5.3.4

This SR requires verification every 31 days of the continuity of two safety-related initiators associated with DC and Uninterruptible AC Electrical Power Distribution Divisions required by LCO 3.8.7, "Distribution Systems - Shutdown," for each required GDCS valve, and for ADS valves required to support relief capacity equivalent to 6 DPVs The 31-day Frequency is acceptable because either of the two safety-related initiators in each valve is capable of actuating the associated GDCS or ADS valve. Additionally, an alarm will provide prompt notification of loss of circuit continuity.

This SR is modified by a Note that continuity is not required to be met for one required initiator intermittently disabled under administrative controls. This allows the continuity monitor to be tested and allows surveillance and maintenance with the assurance that the valve will not be opened inadvertently. The operation of the disable/test switch in either division does not disable the GDCS because the valve will still be opened by the squib initiator in the other division.

SR 3.5.3.5

This SR requires verification every 24 months that that each required GDCS valve and ADS valve required to support relief capacity equivalent to 6 DPVs actuates on an actual or simulated automatic initiation signal. The LOGIC SYSTEM FUNCTIONAL TEST in LCO 3.3.5.2 overlaps this SR to provide complete testing of the assumed safety function.

This SR is modified by two Notes. Note 1 states that for ADS valves this SR is only required to be met in MODE 5 and in MODE 6 prior to removal of the reactor pressure vessel head. ADS is not required for GDCS injection following removal of the reactor pressure vessel head. Note 2 excludes valve actuation as a requirement for this SR to be met. OPERABILITY of required squib-actuated valves is verified by continuity tests and the Inservice Test Program for squib-actuated valves. Required SRVs are tested in accordance with the Inservice Test Program.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The 24-month Frequency for performing this SR is based on the need to perform this SR under the conditions that apply during a plant outage and the potential for an unplanned transient if the SR were performed with the reactor at power. Operating experience has shown that these components usually pass the SR when performed once per the 24-month refueling interval.

SR 3.5.3.6

SR 3.5.3.6 requires the performance of SRs 3.5.2.4 and 3.5.2.5 from LCO 3.5.2. Refer to the corresponding Bases for LCO 3.5.2 for a discussion of each SR.

REFERENCES

1. Chapter 6.
2. Chapter 15.

B 3.5 Emergency Core Cooling Systems (ECCS)

B 3.5.4 Isolation Condenser System (ICS) - Operating

BASES

BACKGROUND

The Isolation Condenser System (ICS) actuates automatically following a reactor pressure vessel (RPV) isolation and transfers sufficient heat from the RPV to the Isolation Condenser/Passive Containment Cooling System IC/PCCS pool to prevent safety relief valve (SRV) actuation (Ref. 1). LCO 3.7.1, “Isolation Condenser/Passive Containment Cooling System (IC/PCCS) Pools,” supports the ICS in removing sufficient decay heat following an RPV isolation to cool the reactor to safe shutdown conditions (MODE 4) within 36 hours and maintain the reactor in a safe condition for an additional 36 hours with minimal loss of RCS inventory (Ref. 1). The ICS also provides water inventory to the RPV at the start of a LOCA and provides the initial RPV depressurization following a loss of feedwater allowing ADS initiation to be delayed. The ICS is also assumed available to respond to a Station Blackout and an Anticipated Transient without Scram (Ref. 1).

The ICS consists of four independent trains. Each ICS train includes a heat exchanger (isolation condenser), a steam supply line that connects the top of the isolation condenser to the RPV, a condensate return line that connects the bottom of the isolation condenser to the RPV, a high point purge line, and vent lines from both the upper and lower headers of the isolation condenser. The isolation condensers are located above the containment and are submerged in a large pool of water (IC/PCCS pool) that is at atmospheric pressure. Steam produced in IC/PCCS pools by boiling around the isolation condenser is vented to the atmosphere (Ref. 1).

Each of the four isolation condensers consists of two identical modules. Each module includes an upper and lower header connected by a bank of vertical tubes. A single vertical steam supply line directs steam from the RPV to the horizontal upper header in each module through four branch lines. The branch lines include flow restrictors that limit the consequences of a line break. Steam is condensed inside banks of vertical tubes that connect the upper and lower headers in each module and the condensate collects in the lower header. Each ICS condensate return line includes an in-line vessel that provides additional water inventory to the RPV when the ICS is initiated.

Operation of each ICS train is initiated by opening either the condensate return valve or the condensate return bypass valve. These valves are in parallel and are both normally closed.

BASES

BACKGROUND (continued)

The condensate return valves open on an ICS initiation signal. The condensate return bypass valves open on loss of power.

With both the condensate return valve and condensate return bypass valves closed and the steam supply line to the reactor open, the isolation condenser and the condensate return line fill with condensate to a level above the upper headers. The steam supply line, which is insulated to prevent the accumulation of condensate, remains filled with steam. A purge line with an orifice connects the top of the isolation condenser to a main steam line. Flow through the purge line when the ICS is in standby prevents the accumulation of non-condensable gases in the top of the isolation condenser.

Upon receipt of an ICS initiation signal, the condensate return valves open causing the condensate in the isolation condenser and condensate return line to return to the RPV. Steam from the RPV continues to condense in the isolation condenser and drains back to the RPV.

Beginning six hours after ICS initiation, radiolytically generated non-condensable gases are automatically, continuously vented to the suppression pool through vent lines connected to the lower header of the isolation condenser. The lower header vent valves also open automatically on high reactor pressure, which could be indicative of a loss of flow through the ICS. Operation of the lower header vent in each train is initiated by opening two, parallel connected, lower header vent valves or, opening two, series connected, lower header vent bypass valves. The lower header vent valves are normally closed, fail-open solenoid-operated valves. One of the valves is controlled by the Safety System Logic and Control /Engineered Safety Features (SSLC/ESF) System described in the Bases for LCO 3.3.5.3, "Isolation Condenser System (ICS) Instrumentation," and LCO 3.3.5.4, "Isolation Condenser System (ICS) Actuation." The other lower header vent valve is controlled by the Diverse Protection System (DPS), which is designed to mitigate digital protection system common mode failures. The lower header vent bypass valves are a relief valve and normally closed, fail-open solenoid valve. The lower header vent bypass valves open automatically (with or without power) at a pressure higher than the lower header vent valves and at a pressure lower than what is needed to lift the SRVs.

Each ICS condenser is located in a sub-compartment of the IC/PCCS pool. Following RPV isolation, pool water temperature could rise to about 101°C (214°F). The steam formed will be non-radioactive and have a

BASES

BACKGROUND (continued)

slight positive pressure relative to station ambient. The steam generated in the IC/PCCS pool is released to the atmosphere through large-diameter discharge vents. Each ICS train is designed to remove 33.75 MWt of decay heat when the reactor is above normal operating pressure so that any three of the four ICS trains have sufficient capacity to perform the ICS design function (Ref. 1).

Each of the condensate return valves is equipped with four solenoids (i.e., initiators). A signal to any of the four initiators will actuate the valve. Three of the four initiators on each valve are actuated by the Safety System Logic and Control /Engineered Safety Features (SSLC/ESF) System described in the Bases for LCO 3.3.5.3, "Isolation Condenser System (ICS) Instrumentation," and LCO 3.3.5.4, "Isolation Condenser System (ICS) Actuation." The fourth initiator is actuated by the Diverse Protection System (DPS), which is designed to mitigate digital protection system common mode failures. The operator is able to stop any individual ICS train whenever the RPV pressure is below a reset value, overriding ICS automatic actuation signals.

Power to each of the three safety-related initiators on each ICS valve is supplied from a different division of the DC and Uninterruptible AC Electrical Power Distribution. As such, at least two of the three initiators in each ICS condensate return valve will be associated with divisions required by LCO 3.8.6, "Distribution Systems - Operating."

Each ICS condenser forms a closed safety-related loop outside the containment that acts as a "passive" substitute for an open "active" valve outside the containment. In addition, the ICS steam supply line and condensate return line each include two, normally open containment isolation valves in series. These valves close automatically to isolate the RPV on indication of a leak or break in the ICS that could bypass the containment. Specifically, high flow indicated on two of the four differential pressure transmitters on each steam supply line or high flow indicated on two of the four differential pressure transmitters on each condensate return line will close all four isolation valves on the associated ICS train. Additionally, elevated radiation levels on two of the four radiation monitors associated with the steam space above each ICS pool subcompartment cause an alarm on radiation levels indicative of a minor leak and will isolate the steam supply and condensate return line of the associated ICS train on radiation levels indicative of a significant leak. Similarly, each ICS purge line also penetrates the containment to the closed system and is equipped with an excess flow check valve and a

BASES

BACKGROUND (continued)

normally open shutoff valve. Each ICS venting line also penetrates the containment to the closed system. The upper header vent line is equipped with two normally closed, fail-closed solenoid valves in series; the lower header vent line is equipped with an excess flow check valve in series with a restricting orifice; and the lower header vent bypass line is equipped with a high-pressure relief valve in series with a normally closed, fail-open solenoid valve.

The ICS isolation valves are also automatically signaled to close upon receipt of an open signal from two or more Depressurization Valves (DPVs). Closing the ICS isolation valves mitigates the accumulation of radiolytic hydrogen and oxygen, and there is sufficient time allotted for the water stored in the ICS condensate line to drain to the RPV prior to the isolation.

The ICS is designed to ensure that no single active component failure will prevent automatic initiation and successful operation of the minimum required ICS subsystems when any three of the four divisions of DC and Uninterruptible AC Electrical Power Distribution and the associated instrumentation divisions are OPERABLE.

APPLICABLE SAFETY ANALYSES

The ICS is assumed to function following an RPV isolation or low water level (Level 2) event (Ref. 1). Operation of three of the four ICS trains after RPV isolation will limit RCS pressure enough to prevent safety relief valve (SRV) actuation. By conserving reactor water inventory following the RPV isolation, ICS minimizes the need for automatic reactor depressurization that would be required to add additional water inventory from low pressure sources.

The ICS also has an ECCS function to provide liquid inventory to the RPV during the initial stages of a LOCA. The ICS also provides the initial depressurization of the reactor during a loss of feed water so that ADS initiation can be delayed.

ICS - Operating satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO	This LCO requires four ICS trains to be OPERABLE. OPERABILITY of each condensate return valve and the SSLC/ESF-actuated lower header vent valve requires OPERABILITY of two safety-related initiators associated with electrical divisions required by LCO 3.8.6. The condensate return bypass valve, the DPS-actuated lower header vent valve, and the lower head vent bypass valves are not required for ICS OPERABILITY. The isolation valve for each ICS condenser subcompartment pool must be locked open. This ensures that the full capacity of the IC/PCCS pools is available to provide required cooling water to the ICS train for at least 72 hours after an RPV isolation or LOCA without the need for operator action. With the ICS subcompartment isolation valve locked open, subcompartment level is maintained in accordance with the requirements in LCO 3.7.1, “Isolation Condenser/Passive Containment Cooling System (IC/PCCS) Pools.”
APPLICABILITY	Four ICS trains are required to be OPERABLE in MODES 1 and 2 and in MODES 3 and 4 when < 2 hours since reactor was critical, to remove reactor decay heat, or provide additional RCS inventory following a LOCA, a loss of feedwater, or a reactor shutdown with isolation. In addition, in MODES 1 and 2, the ICS is required to be OPERABLE to prevent unnecessary automatic reactor depressurization or SRV actuation following RPV isolation or low water level events. ICS requirements in MODES 3 and 4 when ≥ 2 hours since reactor was critical, and in MODE 5 are specified in LCO 3.5.5, “Isolation Condenser System (ICS) - Shutdown.”
ACTIONS	<u>A.1</u> This Condition applies when one of the four ICS trains is inoperable. In this Condition, the remaining three trains have adequate capacity to respond to events described in References 1 and 2. However, the overall reliability is reduced because a failure in one of the OPERABLE trains could result in an insufficient ICS capacity. In this Condition, the inoperable ICS train must be restored to OPERABLE status within 14 days. This Completion Time is acceptable based on engineering judgment considering the low probability of a failure of an additional ICS train concurrent with a design basis event during this period.

BASES

ACTIONS (continued)

B.1

This Condition applies when two or more ICS trains are inoperable. In this condition, the ICS may not have sufficient capacity to respond to events described in References 1 and 2. This Condition also applies when the Required Actions and associated Completion Time of Condition A or B are not met. In this Condition, 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 12 hours. The allowable Completion Time is reasonable, based on plant design, to reach the required unit conditions from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.5.4.1

This SR requires periodic verification that each ICS manual, power-operated, and automatic valve in the flow path, that is not locked, sealed, or otherwise secured in position, is in the correct position. This SR is intended to ensure proper valve alignment in any flow path required for proper operation of the ICS. This SR does not apply to valves that are locked, sealed, or otherwise secured in position, since these were verified to be in the correct position upon locking, sealing, or securing.

This SR does not require any testing or valve manipulation. Rather, it involves verification, through a system walkdown, that those valves outside containment and capable of being mispositioned are in the correct position. The 31-day Frequency for performing this SR is acceptable based on engineering judgment and was chosen to provide added assurance that ICS valves are correctly positioned.

SR 3.5.4.2

This SR requires verification every 31 days that the High Pressure Nitrogen Supply System (HPNSS) pressure to each nitrogen-operated ICS steam supply and condensate return valve is within the specified limit. The 31-day Frequency is acceptable because HPNSS low pressure alarms will provide prompt notification of an abnormal pressure in the HPNSS.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.5.4.3

This SR requires verification every 31 days of the continuity of two safety-related initiators associated with DC and Uninterruptible AC Electrical Power Distribution Divisions required by LCO 3.8.6 for each condensate return valve and each SSLC/ESF-actuated lower header vent valve. The 31-day Frequency is acceptable because either of the two safety-related initiators in each valve is capable of actuating the associated ICS valve. Additionally, an alarm will provide prompt notification of loss of circuit continuity for the required initiators in each ICS valve.

This SR is modified by a Note that continuity is not required to be met for one required initiator intermittently disabled under administrative controls. This allows the continuity monitor to be tested and allows surveillance and maintenance with the assurance that the valve will not be opened inadvertently. The operation of the disable/test switch in either division does not disable the ICS valve because the valve will still be opened by the initiator in the other division.

SR 3.5.4.4

This SR requires periodic verification that each ICS subcompartment manual isolation valve is locked open. This SR ensures that the level in the subcompartment is the same as the level in the associated expansion pool and that the full volume of water in the IC/PCCS pools is available to each condenser. If this SR is not met, the associated ICS train may not be capable of performing its design functions. The 24-month Frequency for this SR is based on engineering judgment and is acceptable because the manual isolation valves between the IC/PCCS pool and the ICS subcompartments are locked open and maintained in their correct position under administrative controls.

SR 3.5.4.5

This SR requires periodic verification that the ICS actuates on an actual or simulated automatic initiation signal. The ICS is required to actuate automatically to perform its design function. This Surveillance test verifies that the automatic initiation logic will cause the ICS to operate as designed when a system initiation signal (actual or simulated) is received. The LOGIC SYSTEM FUNCTIONAL TEST in LCO 3.3.5.4 overlaps this Surveillance to provide complete testing of the assumed ICS function.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The 24-month Frequency for performing this SR is acceptable 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 SR were performed with the reactor at power.

SR 3.5.4.6

This SR requires periodic verification that the heat removal capability of each ICS train satisfies requirements specified in Reference 1. The temperature sensor located downstream of the condensate return isolation valve and the differential pressure transmitter on the condensate return line may be used to provide test data. The Frequency, prior to exceeding 25% RTP if not performed in the previous 24 months on a STAGGERED TEST BASIS, is based on engineering judgment and allows deferring performance until plant conditions needed to perform the test are established.

REFERENCES

1. Section 5.4.6.
2. Section 6.3.3.

B 3.5 Emergency Core Cooling Systems (ECCS)

B 3.5.5 Isolation Condenser System (ICS) - Shutdown

BASES

BACKGROUND

The ICS is designed to operate either automatically or manually following reactor pressure vessel (RPV) isolation to provide adequate RPV pressure reduction to preclude safety relief valve operation and provide core cooling while conserving reactor water inventory (Ref. 1). A description of the ICS is provided in the Bases for LCO 3.5.4, "Isolation Condenser System (ICS) - Operating." When the reactor is shutdown, a reduced ICS capability is maintained to provide cooldown capability and to ensure a highly reliable and passive alternative to the Reactor Water Cleanup/Shutdown Cooling (RWCU/SDC) system for decay heat removal.

RWCU/SDC consists of two independent and redundant trains powered from separate electrical divisions that can be powered from either offsite power or the standby diesel generators. However, RWCU/SDC is a nonsafety-related system that cannot be assumed to remain available following an equipment failure or a loss of offsite power. Depending on plant and equipment status, various alternatives to the RWCU/SDC for decay heat removal can be configured in MODES 3, 4 and 5. When the Isolation Condenser/Passive Containment Cooling System (IC/PCCS) pool and the individual ICS pool subcompartments are flooded, use of one or more ICS loops is the preferred backup method for decay heat removal in MODES 3 and 4.

Although not effective for decay heat removal in MODE 5, the ICS does provide a highly reliable and passive backup to the RWCU/SDC for decay heat removal in this MODE. If normal decay heat removal capability is lost, the reactor coolant temperature will increase until the ICS provides the required decay heat removal capacity.

APPLICABLE SAFETY ANALYSES

A highly reliable, safety-related, and passive alternative to RWCU/SDC for decay heat removal when shutdown is not required for mitigation of any event or accident evaluated in the safety analyses. However, decay heat removal must be accomplished to prevent core damage.

ICS - Shutdown satisfies Criterion 4 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO	This LCO requires that two trains of ICS be OPERABLE when shutdown to provide a backup method for decay heat removal. OPERABILITY of each condensate return valve and the Safety System Logic and Control/Engineered Safety Feature (SSLC/ESF)-actuated lower header vent valve requires OPERABILITY of two safety-related initiators associated with electrical divisions required by LCO 3.8.6. The condensate return bypass valve, the Diverse Protection System (DPS)-actuated lower header vent valve, and the lower head vent bypass valves are not required for ICS OPERABILITY. With the RPV water level above the ICS steam supply line, OPERABILITY of the ICS function is not impacted (Ref. 2). When in MODE 5, required ICS loops require functionality of associated IC/PCCS expansion pools as heat sink for the ICS condensers.
APPLICABILITY	This LCO requires that two trains of ICS be OPERABLE in MODES 3 and 4 when it has been ≥ 2 hours since the reactor was critical, and in MODE 5.
ACTIONS	<u>A.1, A.2, A.3, and A.4</u> If one or more of the required ICS trains are not available, the plant may not have a reliable and passive alternative to RWCU/SDC for decay heat removal. Therefore, action must be taken immediately to restore the required ICS train(s) to operable status. With one of the two required ICS trains inoperable, the remaining train is capable of providing the required decay heat removal. However, the overall reliability is reduced. Therefore, an alternate method of decay heat removal must be provided. With both ICS trains inoperable, an alternate method of decay heat removal must be provided in addition to that provided for the initial ICS train inoperability. The 1-hour Completion Time is based on the decay heat removal function and the probability of a loss of the available decay heat removal capabilities. Furthermore, verification of the functional availability of these alternate method(s) must be reconfirmed every 24 hours thereafter. This will provide assurance of continued decay heat removal capability. The required cooling capacity of the alternate method should be ensured by verifying (by calculation or demonstration) its capability to maintain or

BASES

ACTIONS (continued)

reduce temperature. Decay heat removal by ambient losses can be considered as, or contributing to, the alternate method capability.

Alternate methods that can be used include (but are not limited to) the RWCU/SDC System and the Fuel and Auxiliary Pools Cooling System. With one or more required ICS train(s) inoperable, at least one method of decay heat removal is verified to be in operation. The 1-hour Completion Time is based on engineering judgment recognizing the need to provide decay heat removal. Furthermore, verification must be reconfirmed every 12 hours thereafter. This will provide assurance of continued decay heat removal capability.

During the period when the required ICS train(s) is inoperable, the reactor coolant temperature and pressure must be periodically monitored to ensure proper function of the alternate method. The once per hour Completion Time is deemed appropriate.

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

This Condition applies when the Required Actions and associated Completion Times are not met. In this Condition, action must be initiated immediately to establish reactor building refueling and pool area HVAC subsystem (REPAVS) and contaminated area HVAC subsystem (CONAVS) area isolation boundary. This can be accomplished by isolating the REPAVS and CONAVS dampers or verifying the automatic capability of the respective exhaust high radiation function. This action is needed to establish appropriate compensatory measures for a loss of decay heat removal.

SURVEILLANCE REQUIREMENTS

<u>SR 3.5.5.1</u>

This SR requires verification every 31 days that each ICS manual, power-operated, and automatic valve in the flow path, that is not locked, sealed, or otherwise secured in position, is in the correct position. This SR is intended to ensure proper valve alignment in any flow path required for proper operation of the ICS. This SR does not apply to valves that are locked, sealed, or otherwise secured in position, since these were verified to be in the correct position upon locking, sealing, or securing.

This SR does not require any testing or valve manipulation. Rather, it involves verification, through a system walkdown, that those valves

BASES

SURVEILLANCE REQUIREMENTS (continued)

outside containment and capable of being mispositioned are in the correct position.

The 31-day Frequency for performing this SR is acceptable based on engineering judgment and was chosen to provide added assurance that ICS valves are correctly positioned.

SR 3.5.5.2

This SR requires verification every 31 days that the High Pressure Nitrogen Supply System (HPNSS) pressure to each nitrogen-operated ICS valve is within the specified limit. The 31-day Frequency is acceptable because highly reliable HPNSS low pressure alarms will provide prompt notification of an abnormal pressure in the HPNSS.

SR 3.5.5.3

This SR requires verification every 31 days of the continuity of two safety-related initiators associated with DC and Uninterruptible AC Electrical Power Distribution Divisions required by LCO 3.8.6, "Distribution Systems - Operating," and LCO 3.8.7, "Distribution Systems - Shutdown," for each condensate return valve and each SSLC/ESF-actuated lower header vent valve.

The 31-day Frequency is acceptable because either of the two safety-related initiators in each valve is capable of actuating the associated ICS valve. Additionally, an alarm will provide prompt notification of loss of circuit continuity for the required initiators in each ICS valve.

This SR is modified by a Note that continuity is not required to be met for one required initiator intermittently disabled under administrative controls. This allows the continuity monitor to be tested and allows surveillance and maintenance with the assurance that the valve will not be opened inadvertently. The operation of the disable/test switch in either division does not disable the ICS valve because the valve will still be opened by the initiator in the other division.

SR 3.5.5.4

This SR requires verification every 24 months that each ICS subcompartment manual isolation valve is locked open. This SR is necessary to ensure that the full volume of water in the IC/PCCS pools is available to each condenser. If this SR is not met, the associated ICS

BASES

SURVEILLANCE REQUIREMENTS (continued)

loop may not be capable of performing its design functions. The 24-month Frequency for this SR is based on engineering judgment and is acceptable because the manual isolation valves between the IC/PCCS pool and the ICS subcompartments are locked open and maintained in their correct position under administrative controls.

SR 3.5.5.5

This SR requires verification every 24 months that the ICS actuates on an actual or simulated automatic initiation signal. The ICS is required to actuate automatically to perform its design function. This Surveillance test verifies that the automatic initiation logic will cause the ICS to operate as designed when a system initiation signal (actual or simulated) is received. The LOGIC SYSTEM FUNCTIONAL TEST performed in LCO 3.3.5.4 overlaps this Surveillance to provide complete testing of the assumed ICS function.

The 24-month Frequency for performing this SR is acceptable 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 SR were performed with the reactor at power.

SR 3.5.5.6

SR 3.5.5.6 requires the performance of SR 3.5.4.6 from LCO 3.5.4. Refer to the corresponding Bases for LCO 3.5.4 for a discussion of this SR.

REFERENCES

1. Section 5.4.6.
2. NEDO-33201, ESBWR Certification Probabilistic Risk Assessment, Section 16.4.1, Revision 6, October 2010.

B 3.6 CONTAINMENT SYSTEMS

B 3.6.1.1 Containment

BASES

BACKGROUND

The function of the containment is to isolate and contain fission products released from the reactor coolant system following a design basis loss of coolant accident (LOCA) and to confine the postulated release of radioactive material to within limits. The containment structure is a reinforced concrete cylindrical structure, which encloses the reactor pressure vessel and its related systems and components. The containment structure has an internal steel liner, which provides an essentially leak-tight barrier against an uncontrolled release of radioactive material to the environment.

The isolation devices for the penetrations in the containment boundary are a part of the containment leak tight barrier. To maintain this leak tight barrier:

a. All penetrations required to be closed during accident conditions are either:

   1. Capable of being closed by an OPERABLE automatic containment isolation system or

   2. Closed by manual valves, blind flanges, or de-activated automatic valves secured in their closed positions, except as provided in LCO 3.6.1.3, "Containment Isolation Valves (CIVs),"

b. Containment air locks are OPERABLE, except as provided in LCO 3.6.1.2, "Containment Air Lock,"

c. All equipment hatches are closed, and

d. The sealing mechanism (e.g., welds, bellows, or O-rings) associated with a penetration is OPERABLE.

This Specification ensures that the performance of the containment, in the event of a design basis accident (DBA), meets the assumptions used in the safety analyses of References 1 and 2. SR 3.6.1.1.1 leakage rate requirements are in conformance with 10 CFR 50, Appendix J, Option B (Ref. 3), as modified by approved exemptions.

BASES

APPLICABLE SAFETY ANALYSES

The safety design basis for the containment is that it must withstand the pressures and temperatures of the limiting DBA without exceeding the design leakage rate such that the postulated release of fission-product radioactivity subsequent to a DBA will not result in doses in excess of the values given in the licensing basis.

The DBA that results in a release of radioactive material within containment is a LOCA. In the analysis of this accident, 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.

Analytical methods and assumptions involving the containment are presented in References 1 and 2. The safety analyses assume a non-mechanistic fission-product release following a DBA that forms the basis for determination of offsite doses. The fission-product release is in turn based on an assumed leakage rate from the containment. OPERABILITY of the containment ensures that the leakage rate assumed in the safety analyses is not exceeded, and that the site boundary radiation dose will not exceed the limits of 10 CFR 52.47(a)(2)(iv) and Regulatory Guide 1.183 (Refs. 4 and 5, respectively) even if the non-mechanistic release were to occur.

The maximum allowable leakage rate for the containment (L_a) is 0.35% by weight of the containment air per 24 hours at the maximum calculated containment pressure (Ref. 1), excluding MSIV leakage. The bulk of the containment leakage is released into the reactor building. The remaining portion of primary leakage is assumed to leak through the Passive Containment Cooling System (PCCS) into the airspace directly above the Isolation Condenser/PCCS (IC/PCCS) pools and is quickly vented directly to the atmosphere.

Containment satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO	Containment OPERABILITY is maintained by limiting leakage to ≤ 1.0 L_a, except prior to the first startup after performing a required Containment Leakage Rate Testing Program leakage test. At this time the applicable leakage limits must be met. Additionally, the drywell-to-wetwell gas space leakage must be within acceptance criteria to ensure the pressure suppression function. Compliance with this LCO will ensure a containment configuration, including equipment hatches, that is structurally sound and that will limit leakage to those leakage rates assumed in the safety analysis. Individual leakage rates specified for the containment air locks are addressed in LCO 3.6.1.2.
APPLICABILITY	The containment is required to be OPERABLE in MODES 1, 2, 3, and 4 because 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, containment is not required to be OPERABLE in MODES 5 and 6 to prevent leakage of radioactive material from containment.
ACTIONS	A.1 If the containment is inoperable, a DBA could cause a release of radioactive material to containment. Therefore, the 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 OPERABILITY 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.

BASES

ACTIONS (continued)

B.1 and B.2

If containment cannot be restored to OPERABLE status in 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 12 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 3.6.1.1.1

Maintaining the containment OPERABLE requires compliance with the visual examinations and leakage rate test requirements of the Containment Leakage Rate Testing Program. Failure to meet air lock leakage testing (SR 3.6.1.2.1) or main steam isolation valve leakage (SR 3.6.1.3.9) does not necessarily result in a failure of this SR. The impact of the failure to meet these SRs must be evaluated against the Type A, B, and C acceptance criteria of the Containment Leakage Rate Testing Program. As-left leakage prior to the first startup after performing a required Containment Leakage Rate Testing Program leakage test is required to be < 0.6 L_a for combined Type B and C leakage, and ≤ 0.75 L_a for Option B for overall Type A leakage. At all other times between required leakage rate tests, the acceptance criteria is based on an overall Type A leakage limit of ≤ 1.0 L_a. At ≤ 1.0 L_a the offsite dose consequences are bounded by the assumptions of the safety analysis. The Frequency is required by the Containment Leakage Rate Testing Program.

SR 3.6.1.1.2

This SR measures inleakage past the feedwater flow isolation valves into the containment to ensure that leakage past the feedwater isolation valves is within allowable limits (Ref. 6).

Limiting the leakage from the feedwater system outside containment into the containment is necessary to limit mass water additions to the containment during and following a design basis feedwater line rupture inside containment.

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.

SR 3.6.1.1.3

Maintaining the pressure suppression function of the containment requires limiting the leakage from the drywell to the wetwell. Thus, if an event were to occur that pressurizes the drywell, the steam would be directed through the horizontal vent pipes into the wetwell. This SR measures the wetwell-to-drywell vacuum breaker and vacuum breaker isolation valve pathway leakage to ensure that these leakage paths are within allowable limits.

Satisfactory performance of this SR can be achieved by establishing a known initial differential pressure (≥ 2.0 psid [14 kPaD]) between the drywell side and the wetwell side of the vacuum breaker and isolation valve and verifying that the measured leakage for each is ≤ 15% of the equivalent leakage through an acceptable design basis value $A/\sqrt{K}$ of 2.0 cm^2 (2.16E-03 ft^2). The leakage test is performed every 24 months. The 24-month Frequency is based on the need to perform this Surveillance under the conditions that apply during a plant outage.

The SR is modified by a Note stating that performance of SR 3.6.1.1.5 satisfies this Surveillance Requirement. This is acceptable since SR 3.6.1.5 ensures margin to the design basis pressure suppression function, including the wetwell-to-drywell vacuum breaker leakage. Excluding the isolation valve leakage measurement when performing SR 3.6.1.1.5 introduces minimal added uncertainty based on its role as a backup isolation device and its reliability.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.6.1.1.4

Maintaining the pressure suppression function of the containment requires limiting the leakage from the drywell to the wetwell. Thus, if an event were to occur that pressurizes the drywell, the steam would be directed through the horizontal vent pipes into the wetwell. This SR determines the total wetwell-to-drywell vacuum breaker and vacuum breaker isolation valve pathway leakage (maximum pathway) to ensure that these leakage paths are within allowable limits.

For those outages where the overall drywell-to-wetwell gas space leakage test is not conducted, the vacuum breaker and vacuum breaker isolation valve leakage test verifies that even with the maximum allowable total leakage, a margin of 65% remains for potential passive structural leakage. Historical industry drywell-to-wetwell gas space test data indicates that the leakage through the passive structural components is a small fraction of the remaining 65% margin. The total vacuum breaker leakage limit, combined with negligible leakage from the passive structural area, ensures that the drywell-to-wetwell gas space leakage limit is met for those outages in which the overall drywell-to-wetwell gas space leakage test is not performed.

Satisfactory performance of this SR is achieved by summing the individual wetwell-to-drywell vacuum breaker/vacuum breaker isolation valve pathway leakages (from SR 3.6.1.3) on a maximum pathway basis and verifying that the total measured drywell-to-wetwell gas space leakage is ≤ 35% of the equivalent leakage through an acceptable design basis value $A/\sqrt{K}$ of 2.0 cm^2 (2.16E-03 ft^2). This Surveillance is performed every 24 months. The 24-month Frequency is based on the need to perform this Surveillance under the conditions that apply during a plant outage.

The SR is modified by a Note stating that performance of SR 3.6.1.1.5 satisfies this Surveillance Requirement. This is acceptable since SR 3.6.1.5 ensures margin to the design basis pressure suppression function, including the wetwell-to-drywell vacuum breaker leakage. Excluding the isolation valve leakage measurement when performing SR 3.6.1.1.5 introduces minimal added uncertainty based on its role as a backup isolation device and its reliability.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.6.1.1.5

Maintaining the pressure suppression function of the containment requires limiting the leakage from the drywell to the wetwell. Thus, if an event were to occur that pressurized the drywell, the steam would be directed through the horizontal vent pipes into the wetwell. This SR determines effective overall suppression pool bypass leakage area to ensure that the leakage paths that would bypass the wetwell pressure suppression function are within allowable limits.

Satisfactory performance of this SR can be achieved by establishing a known initial differential pressure (≥ 2.0 psid [14 kPaD]) between the drywell and the wetwell and verifying that the suppression pool bypass leakage equivalent to an area ≤ 50% of the bounding design basis value $A/\sqrt{K}$ of 2.0 cm^2 (2.16E-03 ft^2).

The overall suppression pool bypass leakage test is performed every 24 months. The Frequency is based on the need to perform this Surveillance under the conditions that apply during a plant outage.

REFERENCES

1. Section 6.2.
2. Section 15.4.
3. 10 CFR 50, Appendix J, “Primary Reactor Containment Leakage Testing for Water Cooled Power Reactors.”
4. 10 CFR 52.47(a)(2)(iv).
5. Regulatory Guide 1.183, July 2000.
6. Table 5.4-1.

B 3.6 CONTAINMENT SYSTEMS

B 3.6.1.2 Containment Air Lock

BASES

BACKGROUND

Two double-door containment air locks, one in the upper drywell region and one in the lower drywell region, are built into the containment to provide personnel access to the drywell while maintaining containment isolation during the process of personnel entering and exiting the drywell. The air lock is designed to withstand the same loads, temperatures, and peak design internal and external pressures as the containment (Ref. 1). As part of the containment, the air locks limit the release of radioactive material to the environment during normal plant operation and through a range of incidents up to and including postulated Design Basis Accidents (DBAs).

Each air lock door has been designed and tested to verify its ability to withstand pressures 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 seals and local leakage rate testing capability to ensure pressure integrity. To obtain a leak tight seal, the air lock design uses pressure seated doors (i.e., an increase in containment internal pressure results in increased sealing force on each door).

Each air lock is nominally a right circular cylinder with doors at each end that are interlocked to prevent simultaneous opening. The air lock is provided with limit switches on both doors that provide control room indication of door position. During periods when containment is not required to be OPERABLE, the door interlock mechanism may be disabled, allowing both doors of an air lock to remain open for extended periods when frequent containment entry is necessary. Under some conditions as allowed by this LCO, the containment may be accessed through the air lock when the interlock mechanism has failed by manually performing the interlock function.

The containment air lock forms part of the containment pressure boundary. As such, air lock integrity and air tightness are essential to limit offsite doses from a DBA. Not maintaining air lock integrity or air tightness may result in offsite doses in excess of those described in the plant safety analyses. All leakage rate surveillance requirements conform

BASES

BACKGROUND (continued)

to 10 CFR 50, Appendix J, Option B (Ref. 2), as modified by approved exemptions described in the Containment Leakage Rate Testing Program.

APPLICABLE SAFETY ANALYSES

The DBA that postulates the maximum release of radioactive material within containment is a LOCA. In the analysis of this accident, it is assumed that containment is OPERABLE, such that release of fission products to the environment is controlled by the rate of containment leakage. The containment is designed with an allowable leakage rate of 0.35% by weight of the containment per 24 hours at the calculated maximum containment pressure (Ref. 3), excluding MSIV leakage. This allowable leakage rate forms the basis for the acceptance criteria imposed on the SRs associated with the air lock.

The containment air lock satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

As part of the containment pressure boundary, the air lock’s safety function is related to control of containment leakage rates following a DBA. Thus, the air lock’s structural integrity and leak tightness are essential to the successful mitigation of such an event.

Two containment air locks are required to be OPERABLE. For the air lock to be considered OPERABLE, both air lock doors must be OPERABLE, the air lock interlock mechanism must be OPERABLE, and the air lock must be in compliance with the Type B air lock leakage testing requirements as described in the Containment Leakage Rate Testing Program.

The closure of either the inner or outer door in each air lock is sufficient to provide a leak tight barrier following postulated events. However, both doors are kept closed when the air lock is not being used for normal entry into or exit from containment.

The air lock interlock mechanism allows only one air lock door to be opened at a time. This provision ensures that a gross breach of containment does not exist when the containment is required to be OPERABLE.

BASES

APPLICABILITY

The containment air locks are required to be OPERABLE in MODES 1, 2, 3, and 4 when a DBA could cause a significant increase in containment pressure and the release of radioactive material to containment.

In MODES 5 and 6, the probability and consequences of a LOCA are reduced because RPV pressure and temperature are lower. Therefore, maintaining OPERABILITY of the containment air locks is not required.

ACTIONS

Three Notes modify ACTIONS. Note 1 specifies that entry into and exit from the containment is permissible to perform repairs on the affected air lock. If the outer door is inoperable, then it may be easily accessed to repair. If the inner door is the one that is inoperable, however, then a short time exists when 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 due to 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. The OPERABLE door must be immediately closed after each entry and exit.

Note 2 clarifies that, for this LCO, separate Condition entry is allowed for each air lock. This is acceptable because the Required Actions for each Condition provide appropriate compensatory actions for each inoperable air lock. Complying with the Required Actions may allow for operation to continue. This note clarifies that a subsequent inoperable air lock is governed by the same Condition and associated Required Actions used for the other air lock.

Note 3 provides the clarification that Conditions and Required Actions of LCO 3.6.1.1, “Containment,” are applicable when air lock leakage results in exceeding the overall containment leakage rate acceptance criteria.

<u>A.1, A.2, and A.3</u>

If one air lock door is inoperable, Required Action A.1 specifies that the OPERABLE door must be verified closed and remain closed. This action must be completed within 1 hour. Maintaining the OPERABLE door closed assures that a leak tight containment barrier is maintained by an OPERABLE air lock door. The 1-hour Completion Time is consistent with the Required Actions of LCO 3.6.1.1, “Containment,” which requires that containment be restored to OPERABLE status within 1 hour.

ACTIONS (continued)

Required Action A.2 specifies the air lock must be isolated by locking closed the OPERABLE air lock door within 24 hours. The 24-hour Completion Time is considered reasonable for locking the OPERABLE air lock door because the OPERABLE door is being maintained closed.

Required Action A.3 requires periodic verification that the air lock with an inoperable door has been isolated by the use of a locked closed OPERABLE air lock door. This ensures that an acceptable containment leakage boundary is maintained. The verification interval of 31 days is based on engineering judgment and is considered adequate in view of the administrative controls that make a mispositioned locked door unlikely.

Required Action A.3 is modified by a Note that applies to air lock doors located in high radiation areas and allows these doors to be verified locked closed by use of administrative controls. Allowing verification by administrative controls is considered acceptable, because 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.

Two Notes modify the Required Actions for Condition A. Note 1 ensures that Condition C is entered if both doors in the air lock are inoperable. With both doors in an air lock inoperable, the Action to lock an OPERABLE door closed is not applicable. Required Actions C.1 and C.2 are the appropriate remedial actions.

Note 2 provides an allowance that entry and exit using an inoperable air lock is permissible under the control of a dedicated individual stationed at the air lock to ensure that only one door is opened at a time and that the door does not remain open longer than is required.

<u>B.1, B.2, and B.3</u>

If an air lock door interlock mechanism is inoperable, the Required Actions and associated Completion Times for one inoperable air lock door described for Condition A are applicable.

Two Notes modify the Required Actions. Note 1 ensures that Condition C is entered if both doors in the air lock are inoperable. With both doors in an air lock inoperable, the Action to lock an OPERABLE door closed is not applicable. Required Actions C.1 and C.2 are the appropriate remedial actions.

BASES

ACTIONS (continued)

Note 2 provides an allowance that entry and exit using an inoperable air lock is permissible under the control of a dedicated individual stationed at the air lock to ensure that only one door is opened at a time and that the door does not remain open longer than is required.

Required Action B.3 is modified by a Note that applies to air lock doors located in high radiation areas and allows these doors to be verified locked closed by use of administrative controls. Allowing verification by administrative controls is considered acceptable, because access to these areas is typically restricted. Therefore, the probability of misalignment of the door, once it has been verified to be in the proper position, is small.

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

If the air lock is inoperable for reasons other than those described in Condition A or B, Required Action C.1 specifies that action must be initiated to evaluate containment overall leakage rate using current air lock test results to verify that the requirements of LCO 3.6.1.1 are being met.

Required Action C.2 specifies that the OPERABLE door be verified closed and remain closed. This action must be completed within 1 hour. This specified time period is consistent with the Required Actions of LCO 3.6.1.1, “Containment,” which requires that containment be restored to OPERABLE status within 1 hour.

Required Action C.3 specifies that the air lock must be restored to OPERABLE status within 24 hours. The 24-hour Completion Time is reasonable for restoring an inoperable air lock to OPERABLE status, considering that at least one door in the air lock is maintained closed.

BASES

ACTIONS (continued)

D.1 and D.2

If the inoperable containment air lock cannot be restored 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 12 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 3.6.1.2.1

Maintaining containment air locks OPERABLE requires compliance with the leakage rate test requirements of the Primary Containment Leakage Rate Testing Program. This SR reflects the leakage rate testing requirements with respect to air lock leakage (Type B leakage tests). The periodic testing requirements verify that the air lock leakage does not exceed the allowed fraction of the overall containment leakage rate. The Frequency is specified in the Containment Leakage Rate Testing Program.

Two Notes modify SR 3.6.1.2.1. Note 1 clarifies that an inoperable air lock door does not invalidate the previous successful performance of an overall air lock leakage test. This is acceptable because either air lock door is capable of providing a fission-product barrier in the event of a DBA.

Note 2 specifies that the results of containment air lock leakage rate testing be evaluated as part of the acceptance criteria applicable to SR 3.6.1.1.1.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.6.1.2.2

This SR requires periodic verification that the air lock door interlock will function as designed and that simultaneous inner and outer door opening will not occur inadvertently.

The 24-month Frequency is based on engineering judgment and is acceptable because the interlock mechanism is typically not challenged when containment is entered. Additionally, indications of air lock door status would alert operators promptly of a failure of an interlock.

REFERENCES

1. Section 3.8.
2. 10 CFR 50, Appendix J, "Primary Reactor Containment Leakage Testing for Water-Cooled Power Reactors."
3. Section 6.2.

B 3.6 CONTAINMENT SYSTEMS

B 3.6.1.3 Containment Isolation Valves (CIVs)

BASES

BACKGROUND

The function of CIVs is to limit fission-product release during and following postulated Design Basis Accidents (DBAs) to values less than 10 CFR 52.47(a)(2)(iv) (Ref. 1) offsite dose limits and GDC 19 control room dose limits (Ref. 2). The OPERABILITY requirements for CIVs help ensure that adequate containment leak tightness is maintained during and after an accident by minimizing potential leakage paths to the environment. Containment isolation, within the time limits specified for those isolation valves designed to close automatically, ensures that the release of radioactive material to the environment will be consistent with the assumptions used in the DBA analyses. Therefore, the OPERABILITY requirements provide assurance that containment leakage rates assumed in the safety analyses will not be exceeded.

Containment isolation devices are either passive or active (automatic). Passive devices include manual valves, deactivated automatic valves secured in their closed position (including check valves with flow through the valve secured), blind flanges, and closed systems. Active devices include check valves and automatic valves designed to close following an accident without operator's action.

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 (and possibly loss of containment integrity) or leakage that exceeds limits assumed in the safety analyses. The ESBWR design does not credit any closed system inside containment as a containment barrier.

Main Steam Isolation Valves (MSIVs) and main steamline (MSL) drain isolation valves are actuated by the Reactor Trip and Isolation Function (RTIF) portion of the Leak Detection and Isolation System (LD&IS) as described in Bases for LCO 3.3.6.1, “Main Steam Isolation Valve (MSIV) Instrumentation,” and LCO 3.3.6.2, “Main Steam Isolation Valve (MSIV) Actuation.” Each MSIV is equipped with two safety-related solenoids (i.e., the safety-related initiators). Both MSIV safety-related initiators must de-energize to close the MSIV.

Automatic containment isolation valves (other than MSIVs and MSL drain isolation valves) are actuated by the Safety System Logic and Control/Engineered Safety Features (SSLC/ESF) portion of LD&IS as described in Bases for LCO 3.3.6.3, “Isolation Instrumentation,” and LCO 3.3.6.4, “Isolation Actuation.”

BASES

BACKGROUND (continued)

The automatic containment isolation function of the LD&IS is designed to ensure that no single active component failure will prevent automatic isolation of any containment penetration when any three of the four divisions of DC and Uninterruptible AC Electrical Power Distribution and the associated instrumentation divisions are OPERABLE.

The diverse protection system (DPS) performs selected containment isolation functions as part of the diverse ESF function, which is designed to mitigate digital protection system common mode failures. As described in Bases for LCO 3.3.8.1, "Diverse Protection System," the Reactor Water Cleanup/Shutdown Cooling (RWCU/SDC) System CIVs are required to have OPERABLE diverse isolation capability.

APPLICABLE SAFETY ANALYSES

This LCO was derived from the requirements related to the control of off site radiation doses resulting from major accidents. As delineated in 10 CFR 52.47(a)(2)(iv) (Ref. 1), a proposed site must consider a fission-product release from the core, with offsite release based on the expected demonstrable leakage rate from the containment. As part of the containment boundary, CIV function is essential to containment integrity. Therefore, the safety analysis of any event requiring isolation of containment is applicable to this LCO.

The DBAs that result in a release of radioactive material within containment are a LOCA such as a main feedwater line break, or a main steam line break (MSLB). In the analysis for each of these accidents, it is assumed that CIVs are either closed or close within the required isolation times following event initiation. This ensures that potential leakage paths to the environment through CIVs are minimized. The MSIVs are required to close in ≥ 3 but ≤ 5 seconds; therefore, the 5-second closure time is assumed in the analysis. Likewise, it is assumed that the containment is isolated such that release of fission products to the environment is controlled by the rate of containment leakage.

The DBA analysis assumes isolation of the containment is complete and leakage is terminated, except for the maximum allowable leakage, (L_a). The containment isolation total response time includes signal delay and CIV stroke times. The single-failure criterion required to be imposed in the conduct of plant safety analyses was considered in the design of the containment isolation valves.

BASES

APPLICABLE SAFETY ANALYSES (continued)

The CIVs satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

This LCO requires that each CIV is OPERABLE because CIVs form a part of the containment boundary. The CIV safety function is minimizing offsite radiation exposures resulting from a DBA. This LCO provides assurance that the CIVs will perform their designed safety functions to mitigate the consequences of accidents that could result in offsite exposure.

The automatic power-operated isolation valves are OPERABLE when their isolation times are within limits, the valves actuate on an automatic isolation signal, and excess flow check valves (EFCVs) actuate within the required differential pressure range.

For each automatically actuated CIV, the LCO requires OPERABILITY of required safety-related initiators (e.g., solenoids) associated with DC and Uninterruptible AC Electrical Power Distribution Divisions required by LCO 3.8.6, "Distribution Systems - Operating." For the RWCU/SDC System CIVs, the LCO also requires electrical continuity OPERABILITY of the DPS initiator (i.e., solenoid).

The normally closed isolation valves are OPERABLE when manual valves are closed, automatic valves are deactivated and secured in their closed position, and blind flanges are in place. The normally open manual isolation valves are OPERABLE when they are capable of closing.

The valves covered by this LCO are listed with their associated stroke times (if applicable) in Reference 5.

APPLICABILITY

CIVs must be OPERABLE in MODES 1, 2, 3, and 4 to protect against a DBA release of radioactive material to containment.

In MODES 5 and 6, the probability and consequences of a LOCA are reduced because RPV pressure and temperature are lower. Therefore, OPERABILITY of CIVs is not required to ensure containment integrity when in MODE 5 or 6.

BASES

ACTIONS

The ACTIONS are modified by four Notes. Note 1 allows CIVs to be opened intermittently under administrative controls. These controls consist of stationing a dedicated operator, who is in continuous communication with the control room, at the controls of the valve to isolate the valve when a valid containment isolation signal is indicated.

Note 2 provides clarification that 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 CIV. Complying with the Required Actions may allow for continued operation, and subsequent inoperable CIVs are governed by subsequent Condition entry and application of associated Required Actions.

Note 3 requires that the OPERABILITY of the affected systems be evaluated when a CIV is inoperable. This ensures appropriate remedial actions are taken, if necessary, if the affected system(s) are rendered inoperable by an inoperable CIV. Note 4 specifies that the Conditions and Required Actions of LCO 3.6.1.1, "Containment," are applicable when CIV leakage results in exceeding overall containment leakage rate acceptance criteria when in MODES 1, 2, 3, and 4. Pursuant to LCO 3.0.6, these ACTIONS are not required even when the associated LCO is not met. Therefore, Notes 3 and 4 are added to require the proper actions are taken.

Periodic verification of isolation devices located in high radiation areas may be verified closed by use of administrative means. Allowing verification by administrative means is acceptable because access to these areas is typically restricted. Therefore, the potential for misalignment of these valves, once they have been verified to be in the proper position, is small.

Periodic verification of isolation devices that are locked, sealed, or otherwise secured in position may be verified closed by use of administrative means. Allowing verification by administrative means is considered acceptable, since the function of locking, sealing, or securing components is to ensure that these devices are not inadvertently repositioned. Therefore, the potential for misalignment of these devices, once they have been verified to be in the proper position, is low.

BASES

ACTIONS (continued)

A.1

This Condition applies when one or more RWCU/SDC penetration flow path(s) have an inoperable DPS initiator (i.e., solenoid). In this Condition, required SSLC/ESF initiators will actuate the minimum number of CIVs assumed in the design basis analysis concurrent with any additional single failure.

In this Condition, the inoperable DPS initiator(s) must be restored to OPERABLE status within 30 days. This Completion Time is acceptable because the required safety-related initiators will actuate the minimum number of CIVs required to respond to the design basis LOCA concurrent with any additional single failure.

B.1 and B.2

If one of the CIVs in one or more penetration flow paths is inoperable for reasons other than Condition A or D, the penetration still has isolation capability but the ability to tolerate a single failure is lost. Therefore, Required Action B.1 requires that the affected penetrations must be isolated within 4 hours for penetrations other than the main steam line and within 8 hours for main steam lines.

For penetrations isolated in accordance with Required Action B.1, the valve or device used to isolate the penetration should be the closest to the containment that is available. 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 deactivated automatic valve, a closed manual valve, a check valve with flow through the valve secured, or a blind flange.

The Completion Time of 4 hours to isolate penetrations (other than a main steam line) provides sufficient time to complete the action and is acceptable because the penetration still has isolation capability although the ability to tolerate a single failure is lost.

The Completion Time of 8 hours to isolate a main steam line provides additional time to attempt restoration given that the isolation will result in a transient and the potential for a plant shutdown. This is acceptable because the penetration still has isolation capability although the ability to tolerate a single failure is lost. Continued operation with an isolated main steam line is only permitted if the plant safety analysis allows operation

ACTIONS (continued)

with an isolated main steam line. Such operation must be within the conditions, such as main steam line flow, assumed in the plant safety analysis. For example, justification for plant operation with an MSIV closed must evaluate the potential for significant degradation of components in the reactor and steam systems as a result of acoustic resonance in the active steam lines with increased flow rates. Otherwise, the plant must be placed in cold shutdown.

Required Action B.2 requires periodic verification that isolated penetrations remain isolated. This is necessary to ensure that containment penetrations required to be isolated following an accident, and which are no longer capable of being automatically isolated, will be in the isolation position should an event occur. This Required Action does not require any testing or valve manipulation. Rather, it involves verification that those valves outside containment and capable of potentially being mispositioned are in the correct position. The Completion Time of once per 31 days for verifying each affected penetration is isolated is acceptable because the valves are operated under administrative control and the probability of their misalignment is low.

The Completion Time for verification of isolation valves inside containment is that verification must be completed prior to entering MODE 2 or 4 from MODE 5 if containment was de-inerted while in MODE 5 unless the verification was performed within the previous 92 days. This Completion Time is based on engineering judgment and is acceptable because of the inaccessibility of the valves and other administrative controls that ensure that valve misalignment is unlikely.

C.1

If two or more CIVs are inoperable in one or more penetration flow paths for reasons other than Condition A or D, isolation capability for the penetration may be lost. Therefore, at least one of the CIVs in each flow path must be restored to OPERABLE or Required Action C.1 requires that the penetration be isolated within one hour.

For penetrations isolated in accordance with Required Action C.1, the valve or device used to isolate the penetration should be the closest to the containment available. The method of isolation must include the use of at least one isolation barrier that cannot be adversely affected by a

BASES

ACTIONS (continued)

single active failure. Isolation barriers that meet this criterion are a closed and deactivated automatic valve, a closed manual valve, a check valve with flow through the valve secured, or a blind flange.

The Completion Time of one hour is consistent with the ACTIONS of LCO 3.6.1.1, "Containment," and is reasonable considering the importance of maintaining containment integrity during MODES 1, 2, 3 and 4.

D.1

If MSIV or feedwater line leakage is not within required limits, the assumptions of the safety analysis for the radiological consequences of an event are not met. Therefore, the leakage must be restored to within the required limit.

Restoration of the leakage rate can be accomplished by isolating the penetration that caused the limit to be exceeded by use of one closed and de-activated automatic valve, closed manual valve, or blind flange. When a penetration is isolated, the leakage rate for the isolation penetration is assumed to be the actual pathway leakage through the isolation device(s). If two isolation devices are used to isolate the penetration, the leakage rate is assumed to be the lesser actual pathway leakage of the two devices.

The Completion Time for restoration of MSIV or feedwater line leakage is 8 hours. The Completion Time is consistent with the Completion Time for isolation of an inoperable valve of the same type.

E.1 and E.2

If the Required Action and associated Completion Time is 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 12 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, without challenging plant systems.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.6.1.3.1

This SR requires periodic verification that each 25 mm (1 in), 350 mm (14 in), 400 mm (16 in), and 500 mm (20 in) containment purge valve is closed. This SR ensures that the primary containment purge valves are closed as required or, if open, open for an allowable reason. If a purge valve is open in violation of this SR, the valve is inoperable.

This SR is modified by a Note that permits the 25 mm (1 in), 350 mm (14 in), 400 mm (16 in), and 500 mm (20 in) containment purge valves to be opened for inerting, de-inerting, pressure control, ALARA or air quality considerations for personnel entry, or Surveillances that require the valves to be open.

The 31-day Frequency is based on engineering judgment and has been shown to be acceptable through operating experience. The 31-day Frequency is acceptable because containment purge valve status is available to operations personnel.

SR 3.6.1.3.2

This SR requires periodic verification that each manual CIV and blind flange that is located outside containment and is required to be closed during accident conditions is closed. This SR is not required on valves or blind flanges that are locked, sealed, or otherwise secured. The SR helps to ensure that post-accident leakage of radioactive fluids or gases outside the containment boundary is within design limits.

This SR does not require any testing or valve manipulation. Rather, it involves verification that those valves or blind flanges located outside containment and capable of being mispositioned are in the correct position. In this application, the term "sealed" has no connotation of leak tightness. A sealed valve utilizes a device that provides evidence of unauthorized manipulation (e.g., cable secured by means of a lead seal).

The 31-day Frequency is relatively easy and was chosen to provide added assurance that the valves are in the correct positions. The 31-day Frequency has been shown to be acceptable through operating experience. A Note has been added to this SR to clarify that valves that are open under administrative controls are not required to meet the SR during the time the valves are open.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.6.1.3.3

This SR requires verification every 31 days of the continuity of the RWCU/SDC DPS initiator (i.e., solenoid) and of the required safety-related initiators associated with DC and Uninterruptible AC Electrical Power Distribution Divisions required by LCO 3.8.6 for each CIV.

The 31-day Frequency is acceptable because multiple initiators for each CIV are capable of actuating the associated CIV. Additionally, an alarm will provide prompt notification of loss of circuit continuity for the initiators.

This SR is modified by a Note that continuity is not required to be met for one required initiator circuit intermittently disabled under administrative controls. This allows surveillance and maintenance with the assurance that the CIV will not be inadvertently isolated. The operation of the disable/test switch in one division does not disable the isolation function because of the capability of the remaining required initiator(s).

SR 3.6.1.3.4

This SR requires periodic verification that each manual CIV and blind flange that is 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 valves inside containment, the Frequency defined as “prior to entering MODE 2 or 4 from MODE 5 if containment was de-inerted while in MODE 5 and if not performed within the previous 92 days” is appropriate because these valves and flanges are operated under administrative control and the probability of their misalignment is low. A Note has been added to this SR to clarify that valves that are open under administrative controls are not required to meet the SR during the time the valves are open.

SR 3.6.1.3.5

This SR requires periodic verification that the isolation time of each power-operated and automatic CIV is within required limits. The isolation time test ensures that the valve will isolate in a time period less than or equal to that assumed in the safety analyses. MSIVs are excluded from this SR because MSIV full-closure isolation time is demonstrated by SR 3.6.1.3.6.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The Frequency for this SR is in accordance with the requirements of the Inservice Testing Program.

SR 3.6.1.3.6

This SR requires periodic verification that the isolation time of each MSIV is within the required limits. The isolation time test ensures that the MSIV will isolate in a time period that does not exceed the times assumed in the DBA analyses.

The 24-month Frequency was developed to be consistent with the normal refueling interval and is acceptable based on engineering judgment.

SR 3.6.1.3.7

This SR requires periodic verification that each automatic CIV will actuate to its isolation position on a containment isolation signal. Containment isolation is required to prevent leakage of radioactive material from containment following a DBA. The LOGIC SYSTEM FUNCTIONAL TESTs in LCO 3.3.6.2, LCO 3.3.6.4, and LCO 3.3.8.1 overlap this SR to provide complete testing of the safety function.

This 24-month Frequency was developed to be consistent with the normal refueling interval. This Frequency will allow the SR to be performed during a plant outage because isolation of penetrations could disrupt cooling water flow and the normal operation of critical components.

SR 3.6.1.3.8

This SR requires periodic verification that for a representative sample of reactor instrumentation line EFCVs each reduces flow on a simulated line break. This SR provides assurance that the instrumentation line EFCVs will perform to increase margin to predicted radiological consequences during the postulated instrumentation line break event evaluated in Reference 3.

This 24-month Frequency was developed to be consistent with the normal refueling interval. This interval will allow the SR to be performed during a plant outage because of the potential for an unplanned plant transient if the SR is performed with the reactor at power.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.6.1.3.9

This SR requires periodic verification that the leakage rate through each main steam line is within the specified limit when tested at $\geq P_a$. The analyses in Reference 3 are based on the specified leakage limit.

The MSIV leakage rate must be verified at a frequency in accordance with 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 analyses in Reference 3. Maintaining the MSIVs OPERABLE requires compliance with requirements of 10 CFR 50, Appendix J (Ref. 6), as modified by approved exemptions.

SR 3.6.1.3.10

This SR requires periodic verification that the combined feedwater isolation valves leakage rates for both feedwater line leakage paths is within limits. The leakage rates must be verified in accordance with 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 analyses in References 3 and 4. Maintaining the combined feedwater line leakage paths OPERABLE requires compliance with requirements of 10 CFR 50, Appendix J (Ref. 6), as modified by approved exemptions, which are identified in the Containment Leakage Rate Testing Program.

REFERENCES

1. 10 CFR 52.47(a)(2)(iv).
2. 10 CFR 50, Appendix A, "General Design Criteria for Nuclear Power Plants," GDC 19.
3. Section 15.4.
4. Section 6.2.
5. Section 6.2, Tables 6.2-15 through 6.2-45.
6. 10 CFR 50, Appendix J, "Primary Reactor Containment Leakage Testing for Water-Cooled Power Reactors."

B 3.6 CONTAINMENT SYSTEMS

B 3.6.1.4 Drywell Pressure

BASES

BACKGROUND	The upper limit for containment drywell pressure is an input to the analyses for containment performance during postulated loss-of-coolant accidents (LOCAs). The limit was selected based on plant operating experience as a reasonable upper bound during normal operation. This limitation on drywell pressure provides added assurance that the peak containment pressure does not exceed the design value of 310 kPaG (45.0 psig).
APPLICABLE SAFETY ANALYSES	Containment performance is evaluated for the entire spectrum of break sizes for postulated LOCAs. The upper limit for containment drywell pressure is an initial condition in the analyses (Ref. 1) that ensures that the peak drywell internal pressure will be maintained below the drywell design pressure in the event of a LOCA. The calculated peak drywell pressure for the limiting event is provided in Reference 1. Drywell pressure satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).
LCO	This LCO requires that containment drywell pressure be maintained ≤ 106.9 kPa (15.5 psia) during normal operation. Maintaining containment drywell pressure within the specified limit ensures that an initial condition assumed in the safety analysis remains valid. This ensures that the peak LOCA drywell internal pressure will be maintained below the drywell design pressure in the event of a LOCA.
APPLICABILITY	Containment drywell pressure must be maintained within the specified limit in MODES 1, 2, 3, and 4 when a LOCA could cause a significant increase in containment pressure and the release of radioactive material to containment. In MODES 5 and 6, the probability and consequences of LOCA are reduced because RPV pressure and temperature are lower. Therefore, maintaining drywell pressure within limits is not required when in MODE 5 or 6.

BASES

ACTIONS	A.1 If drywell pressure is not within the limits of the LCO, drywell pressure must be restored 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 Required Actions of LCO 3.6.1.1, “Containment,” which requires that Containment be restored to OPERABLE status within 1 hour. B.1 and B.2 If drywell pressure cannot be restored to within limits in 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 12 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 3.6.1.4.1 This SR requires periodic verification that drywell pressure is within the specified limit. This ensures that facility operation remains within the limits assumed in the containment analysis. The 12-hour Frequency for this SR was developed based on operating experience related to trending of drywell pressure variations and pressure instrument drift during the applicable MODES. The 12-hour Frequency is acceptable because of other indications available in the control room, including drywell pressure alarms, will provide prompt notification of abnormal drywell pressure.
REFERENCES	1. Section 6.2.

B 3.6 CONTAINMENT SYSTEMS

B 3.6.1.5 Drywell Air Temperature

BASES

BACKGROUND	During normal operation, the reactor vessel and piping add heat to the drywell airspace. Drywell coolers remove this energy and maintain appropriate drywell average air temperature. The average airspace temperature affects the calculated response to postulated Design Basis Accidents (DBAs). The limit on drywell average air temperature was developed as a reasonable upper bound based on the plant design and operating plant experience.
APPLICABLE SAFETY ANALYSES	Containment performance is evaluated for the spectrum of break sizes for postulated loss-of-coolant accidents (LOCAs) (Ref. 1). Among the inputs to the design basis analysis is the initial drywell average air temperature (Ref. 1). Analyses assume an initial average drywell air temperature of 46.1°C (115°F). This assumption ensures that the safety analysis utilizes conservative initial conditions. Lower initial temperature represents more initial noncondensable gas mass, and consequently higher long-term analyzed containment pressure. Therefore, the Reference 1 analyses were performed well below the nominal drywell temperature during power operation to ensure conservative peak drywell pressure. Maintaining the operating initial conditions of ≤ 65.5°C (150°F) ensures that the peak post-LOCA drywell long-term temperature does not exceed the maximum allowable temperature of 171°C (340°F) and 121°C (250°F) for the drywell and wetwell, respectively (Ref. 2). The most severe drywell temperature condition occurs as a result of a feedwater line rupture. The maximum calculated drywell average temperature for the worst case break area is provided in Reference 1. Equipment inside containment required to mitigate the effects of a DBA is designed to operate and capable of operating under environmental conditions expected for the accident. Exceeding drywell average air temperature may result in the degradation of the equipment and containment structure under accident loads. Drywell air temperature satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO	This LCO requires that drywell average air temperature be ≤ 65.5°C (150°F). In the event of a DBA, with an initial drywell average temperature less than or equal to the LCO temperature limit, the accident temperature profile assures that the drywell structural temperature is maintained below its design temperature and that required safety related equipment will continue to perform its function.
APPLICABILITY	Drywell average air temperature is required to be within specified limits in MODES 1, 2, 3, and 4. A DBA could cause a release of radioactive material to containment and cause a heatup and pressurization of containment. In MODES 5 and 6, the probability and consequences of a LOCA are reduced because RPV pressure and temperature are lower. Therefore, drywell average temperature within limits is not required in MODE 5 or 6.
ACTIONS	<u>A.1</u> If drywell average air temperature is not within the limit of the LCO, operation may not be within the assumptions of the containment analysis. Therefore, drywell average air temperature must be restored within the specified limit within eight hours. The 8 hour Completion Time provides sufficient time to correct minor problems or to prepare the plant for an orderly shutdown and is acceptable because of the low sensitivity of the analysis to variations in this parameter. <u>B.1 and B.2</u> If the drywell average air temperature cannot be restored within limits 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 12 hours and to MODE 5 within 36 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems

BASES

SURVEILLANCE REQUIREMENTS	SR 3.6.1.5.1 This SR requires verification that drywell average air temperature is within specified limits every 24 hours. Permanently installed temperature sensors are provided in various locations and elevations inside containment. These sensors are fed to the plant computer for averaging and continuous monitoring of the containment. The 24 hour Frequency of the SR is acceptable based on (1) operating experience related to drywell average air temperature variations and temperature instrument drift during the applicable MODES and (2) the low probability of a DBA occurring between surveillances. Furthermore, the 24 hour Frequency is acceptable because highly reliable drywell average air temperature alarms will provide prompt notification of abnormal average air temperature.
REFERENCES	1. Section 6.2. 2. Table 6.2-1.

B 3.6 CONTAINMENT SYSTEMS

B 3.6.1.6 Wetwell-to-Drywell Vacuum Breakers

BASES

BACKGROUND

The function of the wetwell-to-drywell vacuum breakers is to relieve vacuum in the drywell. There are three vacuum breaker flow paths between the drywell and the wetwell, which allow gas flow from the wetwell to the drywell when the drywell is at a negative pressure with respect to the wetwell. Therefore, wetwell-to-drywell vacuum breaker flow paths prevent an excessive negative differential pressure across the wetwell-drywell boundary. Each vacuum breaker is a process-actuated valve, similar to a check valve.

A negative differential pressure across the drywell wall is caused by rapid depressurization of the drywell. Events that cause this rapid depressurization are cooling cycles, inadvertent drywell spray actuation, and steam condensation from sprays or subcooled water reflood of a break in the event of a primary system rupture.

In the event of a primary system rupture, steam condensation within the drywell results in the most severe pressure transient. Following a primary system rupture, the increased pressure inside the drywell forces a mixture of noncondensable gases, steam and water through the vertical/horizontal vent pipes into the suppression pool where the steam is rapidly condensed. Condensation of the steam remaining in the drywell is caused by the ECCS flooding of the RPV and cold water spilling out of the broken pipe directly into the drywell causes depressurization of the drywell.

On the upstream side of the vacuum breaker, a pneumatically operated fail as-is safety-related isolation valve is provided. During a LOCA, when the vacuum breaker opens to equalize the wetwell-to-drywell pressure and subsequently does not completely close as detected by the logic associated with proximity sensors and differential temperature from four groups of divisional thermocouples, a control signal will close the upstream isolation valve to prevent excessive bypass leakage due to the opening created by the vacuum breaker.

BASES

APPLICABLE SAFETY ANALYSES

Analytical methods and assumptions involving the wetwell-to-drywell vacuum breaker flow paths are presented in Reference 1 as part of the accident response of the containment systems. The vacuum breaker flow paths are provided as part of the containment to limit the negative pressure differential across the drywell and wetwell walls that form part of the containment boundary.

A loss of coolant accident (LOCA) could result in excessive negative differential pressure across the wetwell-to-drywell wall, caused by the rapid depressurization of the drywell. The event that results in the limiting rapid depressurization of the drywell is the primary system rupture. Subsequent condensation of the steam would result in depressurization of the drywell.

The Reference 1 safety analyses assume that the vacuum breakers are closed initially and are open at a differential pressure of 3.07 kPa (0.445 psi). The analyses support that one vacuum breaker is sufficient to perform the relief function. The Reference 1 safety analyses also assume that all three vacuum breaker flow paths are isolated when the wetwell and drywell differential pressure is equalized, following the initial vacuum breaker opening. Because failure of a vacuum breaker flow path to isolate could result in excessive bypass leakage that would degrade the pressure suppression capability of the containment, each vacuum breaker flow path is equipped with an isolation valve that will close on a control signal if the associated vacuum breaker does not completely close, as detected by the logic associated with the proximity sensors and differential temperature from four groups of divisional thermocouples. The analyses show that the drywell-to-wetwell design pressure is not exceeded even under the worst-case accident scenario.

The wetwell-to-drywell vacuum breakers and isolation valves satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO	Only two of the three vacuum breaker flow paths must be OPERABLE for opening, with the associated vacuum breaker isolation valves in the open position. All wetwell-to-drywell vacuum breakers, however, are required to be closed (except during testing or when the vacuum breakers are performing their intended design function). Additionally, all vacuum breaker isolation valves must be OPERABLE for automatic closure. Vacuum breaker flow path OPERABILITY provides assurance that the drywell-to-wetwell negative pressure differential remains below the design value. Vacuum breaker flow path OPERABILITY also ensures that there is no excessive bypass leakage should a LOCA occur to maintain the pressure suppression capability of the containment.
APPLICABILITY	Vacuum breaker flow path OPERABILITY must be maintained in MODES 1, 2, 3, and 4 when containment OPERABILITY is required to mitigate the effects of a LOCA. In MODES 5 and 6, the probability and consequences of a LOCA are reduced because RPV pressure and temperature are lower. Therefore, maintaining wetwell-to-drywell vacuum breaker flow paths OPERABLE is not required in MODE 5 or 6 to ensure containment integrity.
ACTIONS	<u>A.1</u> If one required wetwell-to-drywell vacuum breaker flow path is inoperable because its vacuum breaker will not open or the associated isolation valve is not open, the remaining OPERABLE vacuum breaker flow path is capable of providing the vacuum relief function. However, overall system reliability is reduced because a single failure in the remaining vacuum breaker flow path could result in an excessive wetwell-to-drywell differential pressure during a LOCA. Therefore, 7 days is allowed to restore the inoperable wetwell-to-drywell vacuum breaker flow path to OPERABLE for opening status so that plant conditions are consistent with those assumed for the design basis analysis. The Completion Time of 7 days is acceptable because the remaining OPERABLE required wetwell-to-drywell vacuum breaker flow path is capable of providing the vacuum relief function and the low likelihood of a LOCA with a single failure of a vacuum breaker during this period.

BASES

ACTIONS (continued)

B.1

If one wetwell-to-drywell vacuum breaker flow path is inoperable because the vacuum breaker will not close or the associated flow path isolation function is inoperable, there is the potential for containment overpressurization due to this bypass leakage if a LOCA were to occur. An open vacuum breaker flow path allows communication between the drywell and wetwell airspace, degrading the pressure suppression capabilities of the containment. Therefore, the affected wetwell-to-drywell vacuum breaker flow path must be isolated within 8 hours.

C.1

If one wetwell-to-drywell vacuum breaker flow path is inoperable because the vacuum breaker will not close and the associated flow path isolation function is inoperable, there is a high potential for wetwell overpressurization due to bypass leakage if a LOCA were to occur. An open vacuum breaker flow path allows communication between the drywell and wetwell airspace, degrading the pressure suppression capabilities of the containment. Therefore, the affected wetwell-to-drywell vacuum breaker flow path must be isolated within 1 hour.

D.1

If two required wetwell-to-drywell vacuum breaker flow paths are inoperable (i.e., any combination of two of the two required flow paths for opening and the three flow paths for the isolation function), there is a high potential that an excessive wetwell-to-drywell differential pressure could exist during a LOCA, or for degradation of the pressure suppression capabilities of the containment. Therefore, one required wetwell-to-drywell vacuum breaker flow path must be restored to OPERABLE status within 1 hour.

BASES

ACTIONS (continued)

E.1 and E.2

If the Required Action and associated Completion Time 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 12 hours and MODE 5 within 36 hours. The allowed Completion Times are reasonable, based on plant design, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.6.1.6.1

This SR requires periodic verification that each vacuum breaker is closed to ensure that this potential large bypass leakage path is not present. This SR is performed by observing the vacuum breaker position indication.

The 14 day Frequency is based on engineering judgment and has been shown to be acceptable through operating experience. The 14 day Frequency is acceptable because vacuum breaker status is available to operations personnel and a highly reliable alarm will alert operations personnel of abnormal vacuum breaker position or valve alignment.

SR 3.6.1.6.2

This SR requires periodic verification that the vacuum breaker isolation valve associated with the two required vacuum breaker flow paths are open.

The 31 day Frequency is based on engineering judgment and has been shown to be acceptable through operating experience.

SR 3.6.1.6.3

This SR requires periodic verification of the free movement of the two required vacuum breakers by verifying that the force required to open each vacuum breaker is within limits to ensure they are capable of performing their intended function.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The 24 month Frequency was developed to coincide with the 24 month refueling interval because access to the vacuum breakers is required to perform the SR. The 24 month Frequency is acceptable based on the simplicity and reliability of the valve design. Specifically, the design of the ESBWR vacuum breaker has been enhanced by eliminating the actuator and the associated failure mode, improving the valve hinge design, and selecting materials which are resistant to wear and galling.

SR 3.6.1.6.4

CHANNEL CALIBRATION is a complete check of the instrument loop and the sensor. This test verifies that the channel responds to the measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to the required nominal trip setpoint within the "as-left tolerance" to account for instrument drifts between successive calibrations consistent with the methods and assumptions required by the Setpoint Control Program. The 24 month Frequency was developed to coincide with the 24 month refueling interval because access to the vacuum breakers is required to perform the SR.

SR 3.6.1.6.5

A system functional test is performed to ensure that each vacuum breaker flow path isolation function operates as required. This includes verifying that the isolation valve automatically closes when the associated vacuum breaker does not completely close, as detected by the logic associated with proximity switches and differential temperature from four groups of divisional thermocouples. The 24 month Frequency was developed to coincide with the 24 month refueling interval based on the need to perform this Surveillance under the conditions that apply during a plant outage.

REFERENCES

1. Section 6.2.

B 3.6 CONTAINMENT SYSTEMS

B 3.6.1.7 Passive Containment Cooling System (PCCS)

BASES

BACKGROUND

The Passive Containment Cooling System (PCCS) is designed to transfer heat from the containment drywell to the Isolation Condenser/PCCS (IC/PCCS) pools following a loss of coolant accident (LOCA). The PCCS consists of six independent condensers. Each condenser is a heat exchanger that is an integral part of the containment pressure boundary. The condensers are located above the containment and are submerged in a large pool of water (IC/PCCS pool) that is at atmospheric pressure. Steam produced in IC/PCCS pools by boiling around the PCCS condensers is vented to the atmosphere. LCO 3.7.1, “Isolation Condenser/Passive Containment Cooling System (IC/PCCS) Pools,” supports the PCCS in removing sufficient post-LOCA decay heat from the containment to maintain containment pressure and temperature within design limits for a minimum of 72 hours, without operator action (Ref. 1)

Each of the six PCCS condensers consists of two identical modules. A single central steam supply pipe, open to the drywell at its lower end, directs steam from the drywell to the horizontal upper header in each module. Steam is condensed inside banks of vertical tubes that connect the upper and lower header in each module. The condensate collects in each module’s lower header and drain volume and then returns by gravity flow to the Gravity-Driven Cooling System (GDCS) pools. By returning the condensate to the GDCS pools, it is available to return to the reactor pressure vessel (RPV) via the GDCS injection lines. Noncondensable gases that collect in the condensers during operation are purged to the suppression pool via vent lines. To reduce accumulation of radiolytic gas in the PCCS vent lines, vent line catalyst modules composed of metal parallel plates coated with catalyst are placed near the entrance of each vent line. Back-flow from the GDCS pool to the suppression pool is prevented by a loop seal in the GDCS drain line.

The RPV is contained within the drywell so that drywell pressure rises above the pressure in the wetwell (suppression pool) during a LOCA. This differential pressure initially directs the high energy blowdown fluids from the RPV break in the drywell through both the pressure suppression pool and through the PCCS condensers. As the flow passes through the PCCS condensers, heat is rejected to the IC/PCCS pool, thus cooling the containment.

BASES

BACKGROUND (continued)

There are no isolation valves on the PCCS inlets from the drywell, or the drain lines to the GDCS pools, or the vent lines to the suppression pool. The PCCS does not have instrumentation, control logic, or power-actuated valves, and does not need or use electrical power for its operation in the first 72 hours after a LOCA. This configuration makes the PCCS fully passive because no active components are required for the system to perform its design function (Ref. 2). Long-term effectiveness of the PCCS (beyond 72 hours) is supported by a vent fan that is connected to each PCCS vent line and exhausts to the GDCS pool. The PCCS vent fans aid in the long-term removal of non-condensable gas from the PCCS for continued condenser efficiency.

Spectacle flanges in the suppression pool vent line and the GDCS drain line are used to isolate the condensers to allow post maintenance leakage tests separately from Type A containment leakage tests.

Each PCCS condenser is located in a sub-compartment of the IC/PCCS pool. During a LOCA, pool water temperature could rise to about 102°C (216°F) (Ref. 1). The steam formed will be non-radioactive and have a slight positive pressure relative to station ambient. The steam generated in the IC/PCCS pool is released to the atmosphere through large-diameter discharge vents. A moisture separator is installed at the entrance to the discharge vent lines to preclude excessive moisture carryover and loss of IC/PCCS pool water.

Each PCCS condenser is designed to remove a minimum 7.8 MWt of decay heat assuming the containment side of the condenser contains pure, saturated steam at 308 kPa absolute (45 psia) and 134°C (273°F); and, the IC/PCCS pool is at atmospheric pressure with a water temperature of 102°C (216°F).

APPLICABLE SAFETY ANALYSES

Reference 1 contains the results of analyses used to predict containment pressure and temperature following large and small break LOCAs. The intent of the analyses is to demonstrate that the heat-removal capacity of the Passive Containment Cooling System is adequate to maintain the containment conditions within design limits. The time history for containment pressure and temperature are calculated to demonstrate that the maximum values remains below the design limit.

PCCS satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO	This LCO requires six PCCS condensers to be OPERABLE. OPERABILITY of a PCCS condenser requires that all the performance and physical arrangement SRs for the PCCS condensers be met. Additionally, the isolation valve for the PCCS condenser subcompartment pool must be locked open. This ensures that the full capacity of the IC/PCCS pools is available to provide required cooling water to the PCCS condenser for at least 72 hours after a LOCA without the need for operator action. With the PCCS subcompartment isolation valve locked open, subcompartment level is maintained in accordance with the requirements in LCO 3.7.1, "Isolation Condenser/Passive Containment Cooling System (IC/PCCS) Pools."
APPLICABILITY	The PCCS condensers are required to be OPERABLE in MODES 1, 2, 3, and 4 because a LOCA could cause a pressurization and heat up of containment. In MODES 5 and 6, the probability and consequences of a LOCA are reduced because of the pressure and temperature limitations of these MODES. Therefore, passive containment cooling is not required to be OPERABLE in MODES 5 and 6.
ACTIONS	<u>A.1</u> If one or more PCCS condensers are inoperable, the functional capability of the passive containment cooling is degraded. All six PCCS condensers must be made OPERABLE within 8 hours to ensure that containment cooling capacity is maintained. The Completion Time is based on engineering judgment considering the low probability of an event requiring PCCS operation. <u>B.1 and B.2</u> If the Required Action and Completion Time of Condition A are not met, functional capability of the passive containment cooling is assumed lost. Therefore, 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 12 hours and to MODE 5 within 36 hours. The Completion Time is reasonable, based on plant design, to reach required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.6.1.7.1

This SR requires periodic verification that the spectacle flanges for the vent, and drain line for each PCCS condenser are in the free flow position. This SR is required to ensure that each PCCS condenser is aligned to function properly when required.

Performance of the SR requires entry into containment. Therefore, this SR is performed prior to entering MODE 2 or 4 from MODE 5 if containment was de-inerted while in MODE 5 unless the SR was performed in the previous 92 days. This Frequency is acceptable because changing the status of the PCCS spectacle flanges requires entry into containment, is performed under administrative controls during planned maintenance activities, and is unlikely to occur inadvertently.

SR 3.6.1.7.2

This SR requires verification every 24 months that each PCCS subcompartment manual isolation valve is locked open. This SR ensures that the level in the subcompartment is the same as the level in the associated expansion pool and that the full volume of water in the IC/PCCS pools is available to each condenser. If this SR is not met, the associated PCCS condenser may not be capable of performing its design function. The 24-month Frequency is based on engineering judgment and is acceptable because the manual isolation valves between the IC/PCCS pool and the PCCS subcompartments are locked open and maintained in their correct position under administrative controls.

SR 3.6.1.7.3

This SR requires periodic verification that both modules in each PCCS condenser have an unobstructed path from the drywell inlet through the condenser tubes to both the GDCS pool through the drain line and to the suppression pool through the vent line.

The Frequency for this SR is 24 months on a STAGGERED TEST BASIS for each PCCS condenser. This Frequency requires testing one of the six PCCS condensers every 24 months, which is consistent with the normal refueling interval. The Frequency is based on engineering judgment, the simplicity of the design, and the requirement for containment access to perform the SR.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.6.1.7.4

This SR requires visual examination of each PCCS vent catalyst module and verification that there is no evidence of abnormal conditions.

The Frequency for this SR is 24 months on a STAGGERED TEST BASIS for each PCCS condenser. This frequency requires testing two of twelve vent catalyst modules every 24 months, which is consistent with the typical refueling cycle. The Frequency is based on engineering judgment, the simplicity of the design, the inerted conditions which the catalyst modules will be exposed to in their standby mode, and the requirement to access containment to perform the SR.

SR 3.6.1.7.5

This SR requires verifying performance of a representative sample of PCCS vent catalyst module plates.

The Frequency for this SR is 24 months on a STAGGERED TEST BASIS for each PCCS condenser. This Frequency requires testing two of twelve vent catalyst modules every 24 months, which is consistent with the typical refueling cycle. The Frequency is based on engineering judgment, the simplicity of the design, the inerted conditions which the catalyst modules will be exposed to in their standby mode, and the requirement to access containment to perform the SR. The representative sample consists of one plate from each PCCS vent catalyst module.

REFERENCES

1. Chapter 6.
2. Chapter 19.

B 3.6 CONTAINMENT SYSTEMS

B 3.6.1.8 Containment Oxygen Concentration

BASES

BACKGROUND	All nuclear reactors must be designed to withstand events that generate hydrogen either due to the zirconium metal water reaction in the core or due to radiolysis. The primary method to control hydrogen is to inert the containment to meet 10 CFR 50.44(c)(2). With the containment inert, that is, oxygen concentration < 4.0 volume percent (v/o), a combustible mixture cannot be present in the containment for any hydrogen concentration. An event that rapidly generates hydrogen from zirconium metal water reaction could result in excessive hydrogen in containment, but oxygen concentration will remain < 4.0 v/o and no combustion can occur. This LCO ensures that oxygen concentration does not exceed 4.0 v/o during operation in the applicable conditions.
APPLICABLE SAFETY ANALYSES	The Reference 1 calculations assume that the containment is inerted when a Design Basis Accident (DBA) loss of coolant accident (LOCA) occurs. Thus, the hydrogen assumed to be released to the containment as a result of metal water reaction in the reactor core will not produce combustible gas mixtures in the containment. The safety analyses show that the core does not uncover during the DBA LOCA and as a result, there is no fuel damage or fuel clad-coolant interaction leading to significant hydrogen generation that would result in a combustible gas condition (Ref. 1). Therefore, containment oxygen concentration does not satisfy any of the 10 CFR 50.36(c)(2)(ii) criteria. This LCO is included in accordance with NRC guidance provided in Reference 2.
LCO	The containment oxygen concentration is maintained < 4.0 v/o to maintain acceptable risk mitigation of combustible gases produced by beyond design-basis accidents involving both fuel-cladding oxidation and core-concrete interaction. The intent is to ensure that an event that produces any amount of hydrogen does not result in a combustible mixture inside primary containment.

BASES

APPLICABILITY	The containment oxygen concentration must be within the specified limit, except as allowed by the relaxations during startup and shutdown addressed below. The containment must be inert with THERMAL POWER > 15% RTP, since this is the condition with the highest probability of an event that could lead to significant hydrogen generation. Inerting the containment is an operational problem because it prevents containment access without an appropriate breathing apparatus. Therefore, the containment is inerted as late as possible in the plant startup and de-inerted as soon as possible in the plant shutdown. When operating with THERMAL POWER ≤ 15% RTP, the potential for an event that generates significant hydrogen is low and the containment need not be inert. Furthermore, the probability of an event that generates hydrogen occurring within the first 24 hours of a startup, or within the last 24 hours before a shutdown, is low enough that these "windows," when the containment is not inerted, are also justified. The 24-hour time period is a reasonable amount of time to allow plant personnel to perform post-startup inspections, as well as inerting or de-inerting.
ACTIONS	A.1 If oxygen concentration is ≥ 4.0 v/o at any time while operating with THERMAL POWER > 15% RTP, with the exception of the relaxations allowed during startup and shutdown, oxygen concentration must be restored to < 4.0 v/o within 24 hours. The 24-hour Completion Time is allowed when oxygen concentration is ≥ 4.0 v/o based on engineering judgment considering the low probability and long duration of an event that would generate significant amounts of hydrogen occurring during this period. B.1 If oxygen concentration cannot be restored to within limits within the required Completion Time, the plant must be brought to a MODE or other specified condition in which the LCO does not apply. To achieve this status, THERMAL POWER must be reduced to ≤ 15% RTP within 8 hours. The 8-hour Completion Time is reasonable, based on operating experience, to reduce reactor power from full power conditions in an orderly manner and without challenging plant systems.

BASES

SURVEILLANCE REQUIREMENTS	SR 3.6.1.8.1 The containment must be determined to be inert by verifying that oxygen concentration is < 4.0 v/o. The 7-day Frequency is based on the slow rate at which oxygen concentration can change and on other indications of abnormal conditions (which would lead to more frequent checking by operators in accordance with plant procedures). Also, this Frequency has been shown to be acceptable through operating experience.
REFERENCES	1. Section 6.2.5. 2. NRC letter, Manny Comar to General Electric Company, "Request for Additional Information Letter No. 107 Related to ESBWR Design Certification Application," dated August 31, 2007.

B 3.6 CONTAINMENT SYSTEMS

B 3.6.2.1 Suppression Pool Average Temperature

BASES

BACKGROUND

The wetwell is a reinforced concrete vessel containing a volume of water called the suppression pool. The suppression pool is designed to absorb the energy associated with decay heat and sensible energy released during a reactor blowdown from Safety Relief Valve (SRV) discharges or from Design Basis Accidents (DBAs). The suppression pool must quench all the steam released through the vent lines during a loss-of-coolant accident (LOCA). This is the essential mitigative feature of a pressure suppression containment that ensures that the peak containment pressure is maintained below the design pressure for DBAs of 310 kPaG (45 psig). Suppression pool average temperature (along with LCO 3.6.2.2, “Suppression Pool Water Level”) is a key indication of the capacity of the suppression pool to fulfill these requirements.

The technical concerns that lead to the development of suppression pool average temperature limits are as follows:

a. Assure steam condensation of the blowdown,

b. Assure containment peak pressure and temperature are below design values, and

c. Assure steam condensation loads are acceptable.

APPLICABLE SAFETY ANALYSES

The postulated DBA against which containment performance is evaluated is the entire spectrum of postulated pipe breaks within the containment. Inputs to the safety analyses include initial suppression pool water volume and suppression pool temperature (Ref. 1 for LOCAs, and Reference 2 for stuck open relief valve).

An initial pool temperature of 43.3°C (110°F) is assumed for the Reference 1 and Reference 2 analyses. Reactor shutdown at a pool temperature of 48.9°C (120°F) and vessel depressurization at a pool temperature of 54.4°C (130°F) are also assumed.

Suppression pool average temperature satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO

This LCO establishes the following limits for suppression pool average temperature:

a. When THERMAL POWER is > 1% RTP and testing which adds heat to the suppression pool is not being performed, average temperature must be ≤ 43.3°C (110°F). This requirement ensures that licensing bases initial conditions are met.

b. When THERMAL POWER is > 1% RTP and testing which adds heat to the suppression pool is being performed, average temperature must be ≤ 46.1°C (115°F). This requirement ensures that the plant has testing flexibility and was selected to provide margin below the 48.9°C (120°F) limit at which reactor shutdown is required. When testing ends, temperature must be restored to ≤ 43.3°C (110°F) within 24 hours per Required Action A.2.

c. When THERMAL POWER is ≤ 1% RTP, average temperature must be ≤ 48.9°C (120°F). This requirement ensures that licensing bases initial conditions are met.

A limitation on the suppression pool average temperature is required to ensure that the containment conditions assumed for the safety analyses are met. This limitation is necessary so that peak containment pressures and temperatures predicted by the safety analyses do not exceed maximum allowable values during a postulated DBA or any transient that results in heatup of the suppression pool.

APPLICABILITY

Suppression pool average temperature must be maintained within specified limits in MODES 1, 2, 3, and 4 when a DBA could cause significant heatup of the suppression pool.

In MODES 5 and 6, the probability and consequences of a LOCA are reduced because Reactor Pressure Vessel (RPV) pressure and temperature are lower. Therefore, maintaining suppression pool average temperature within limits is not required in MODES 5 or 6 to ensure containment integrity.

BASES

ACTIONS

A.1 and A.2

If suppression pool average temperature is > 43.3°C (110°F) but ≤ 48.9°C (120°F), and THERMAL POWER is > 1% RTP, and testing that adds heat to the suppression pool is not being performed, then the requirements of LCO 3.6.2.1.a are not being met. Therefore, Required Action A.2 requires that suppression pool average temperature be restored to within required limits within 24 hours. Additionally, Required Action A.1 requires verification every hour that suppression pool average temperature has not exceeded limits specified in LCO 3.6.2.1.c because this temperature would require immediate entry into condition D.

The Completion Time of 24 hours to restore the temperature to within the limits of LCO 3.6.2.1.a is acceptable because significant containment cooling capability still exists and the containment pressure suppression function will occur at temperatures well above those assumed for safety analyses. Therefore, continued operation is allowed for a limited time. Additionally, the 24-hour Completion Time is adequate to allow the suppression pool temperature to be restored below the limit.

The Completion Time of once per hour for verification that the limits specified in LCO 3.6.2.1.c have not been exceeded is acceptable because experience has shown that pool temperature increases relatively slowly when not performing testing that adds heat to the pool. Furthermore, other indications in the control room will alert the operator to an abnormal suppression pool temperature trend and alarms will alert operators if specified limits are exceeded.

B.1

If the Required Actions and associated Completion Times of Condition A not met, suppression pool average temperature has not been restored to within limits in the required Completion Time. Therefore, the plant must be placed in a MODE in which the LCO 3.6.2.1.a does not apply. This is accomplished by reducing power to ≤ 1% RTP within 12 hours. The 12-hour Completion Time is reasonable, based on operating experience, to reduce reactor power from full power conditions in an orderly manner and without challenging plant systems.

C.1

If suppression pool average temperature is > 46.1°C (115°F), THERMAL POWER is > 1% RTP, and testing that adds heat to the suppression pool is being performed, the temporary allowance provided for suppression

BASES

ACTIONS (continued)

pool heating for testing has been exceeded. Therefore, all testing must be immediately suspended to preserve the heat absorption capability of the pool. When the testing suspended, Condition A is entered and the Required Actions and associated Completion Times are applicable.

D.1, D.2 and D.3

If suppression pool average temperature is > 48.9°C (120°F), an automatic reactor shutdown is initiated because suppression pool temperature exceeds safety analyses assumptions. Therefore, Required Action D.1 specifies placing the reactor mode switch in the shutdown position as a manual backup to the automatic function.

If the reactor is shutdown and suppression pool average temperature > 48.9°C (120°F), the requirements of LCO 3.6.2.1.c are still not met. Therefore, Required Action D.2 requires monitoring suppression pool average temperature every 30 minutes because of the degraded capacity of the suppression pool. This completion time is acceptable because other indications in the control room will alert the operator to abnormal suppression pool temperature trends and alarms will alert operators if specified limits are exceeded. Additionally, 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 5 within 36 hours.

E.1

If suppression pool average temperature is > 54.4°C (130°F), the capacity of the suppression pool is significantly degraded. Therefore, the plant must be placed in a condition in which overall plant risk is reduced. This is accomplished by placing the plant in at least MODE 5 within 12 hours. The allowed Completion Time ensures that the plant is promptly placed in a MODE in which the suppression pool is not required.

SURVEILLANCE REQUIREMENTS

SR 3.6.2.1.1

This SR requires verification that suppression pool average temperature is within specified limits every 24 hours. The average temperature is determined automatically by instrumentation that takes an average of OPERABLE suppression pool water temperature channels.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The 24-hour Frequency for this SR is based on operating experience related to trending suppression pool average temperature changes and instrument drift during the applicable MODES and the need for assessing the proximity to the specified limits. The 24-hour Frequency is acceptable because highly reliable suppression pool temperature alarms will provide prompt notification of abnormal suppression pool average temperature.

REFERENCES

1. Section 6.2.
2. Chapter 15.

B 3.6 CONTAINMENT SYSTEMS

B 3.6.2.2 Suppression Pool Water Level

BASES

BACKGROUND	The wetwell is a reinforced concrete vessel containing a volume of water called the suppression pool. The suppression pool is designed to absorb the energy associated with decay heat and sensible heat released during a reactor blowdown from Safety Relief Valve (SRV) discharges or from a Design Basis Accident (DBA). The suppression pool must quench all the steam released through the vent lines during a loss-of-coolant accident (LOCA). This is the essential mitigative feature of a pressure suppression containment, which ensures that the peak containment pressure during a DBA is maintained below the design pressure of 310 kPaG (45 psig). The suppression pool water volume is approximately 4424 m^3 (156,200 ft^3) at the normal water level of 5.45 m (17.9 ft) above pool floor.
APPLICABLE SAFETY ANALYSES	The upper and lower limits for suppression pool water level are inputs to the analyses for containment performance during postulated accidents and transients. Suppression pool level affects suppression pool temperature response calculations, calculated drywell pressure during vent clearing for a DBA, calculated loads due to a DBA LOCA, and calculated loads due to SRV discharges. Suppression pool water level must be maintained within the limits specified so that the safety analysis of Reference 1 remains valid. If suppression pool water level is too low, insufficient water is available to adequately condense the steam from the SRV quenchers and the main vents. The lower volume would absorb less steam energy before heating up excessively. The Passive Containment Cooling System (PCCS) vent return lines must also be submerged. Therefore, a minimum pool water level is specified. If suppression pool water level is too high, it could result in excessive clearing loads from SRV discharges and excessive hydrodynamic loads due to a DBA LOCA. Therefore, a maximum pool water level is specified. This LCO specifies an acceptable range to prevent the suppression pool water level from being either too high or too low.

BASES

APPLICABLE SAFETY ANALYSES (continued)

Suppression pool water level satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

This LCO requires that suppression pool water level be maintained ≥ 5.4 meters (17.7 feet) and ≤ 5.5 meters (18.0 feet) above the pool floor. These limits ensure that the initial conditions assumed for the safety analyses for containment are met.

APPLICABILITY

Suppression pool water level must be maintained within specified limits in MODES 1, 2, 3, and 4 when a DBA could cause significant loads on the containment. In MODES 5 and 6, the potential for SRV actuation is eliminated and the probability and consequences of LOCA are reduced because RPV pressure and temperature are lower. Therefore, maintaining suppression pool level within limits is not required to ensure containment integrity when in MODE 5 or 6.

ACTIONS

A.1

If suppression pool water level is not within specified limits, the initial conditions assumed for the safety analyses are not met. Therefore, suppression pool water level must be restored to within specified limits within 2 hours. This Completion Time is expected to be sufficient to restore suppression pool water level.

The 2-hour Completion Time is acceptable because the pressure suppression function still exists as long as the main vents, SRV quenchers, and PCCS vent return lines are covered even if water level is below the minimum level. Additionally, protection against overpressurization may still exist due to the margin in the peak containment pressure analysis even if water level is above the maximum level. This Completion Time also takes into account the low probability of an event during this interval.

BASES

ACTIONS (continued)

B.1 and B.2

If the Required Action and Completion Time of Condition A are not met, 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 12 hours and to MODE 5 within 36 hours. The Completion Time is reasonable, based on plant design, to reach required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.6.2.2.1

This SR requires verification that suppression pool water level in within specified limits every 24 hours. The 24-hour Frequency for this SR is based on operating experience related to trending suppression pool water level variations and water level instrument drift during the applicable MODES and the need for assessing the proximity to the specified limits. The 24-hour Frequency is acceptable because suppression pool level alarms will provide prompt notification of abnormal suppression pool level.

REFERENCES

1. Chapter 6.

B 3.6 CONTAINMENT SYSTEMS

B 3.6.3.1 Reactor Building (Contaminated Area Ventilation Subsystem (CONAVS) Area)

BASES

BACKGROUND

The Reactor Building (RB) is a reinforced concrete structure that completely surrounds the containment (except the basemat). The RB provides an added barrier to fission product release from the containment during an accident; contains, dilutes, and holds up any leakage from the containment; and, houses safety-related systems.

The ESBWR design does not include a secondary containment; however, credit is taken for the existence of the RB Contaminated Area Ventilation Subsystem (CONAVS) areas surrounding the primary containment vessel in radiological analyses. RB HVAC system performs no safety-related function, other than the building ventilation isolation function, but credit is taken for hold up in the RB CONAVS area volume as discussed in Reference 1. The radiological dose consequences for LOCAs are based on an assumed containment leak rate of 0.35 weight percent per day. The bulk of the containment leakage is released into the RB (CONAVS area) and the RB (CONAVS area) leaks to the environment at a maximum rate of 211 scfm (Ref. 2). The remaining portion of primary leakage is assumed to leak through the Passive Containment Cooling System (PCCS) into the airspace directly above the Isolation Condenser/PCCS (IC/PCCS) pools and is quickly vented directly to the atmosphere.

The RB (CONAVS area) envelops all penetrations through the containment (except penetrations for MSIV and feedwater lines located in the main steam tunnel and IC/PCCS pools). Under accident conditions, the CONAVS area of the RB is isolated or passively sealed (e.g., water loop seals) to provide a hold up barrier. Therefore, containment isolation valve leakage as well as penetration leakage collects in the RB (CONAVS area). With low leakage and stagnant conditions, the RB (CONAVS area) provides a significant volume for hold up to enhance the basic mitigating functions provided by containment.

Automatic RB (CONAVS area) isolation dampers (other than MSIVs) are actuated by the Safety System Logic and Control/Engineered Safety Features (SSLC/ESF) portion of LD&IS as described in Bases for LCO 3.3.6.3, “Isolation Instrumentation,” and LCO 3.3.6.4, “Isolation Actuation.” The automatic RB (CONAVS area) isolation function of the

BASES

BACKGROUND (continued)

LD&IS is designed to ensure that no single active component failure will prevent automatic isolation of the CONAVS area when any three of the four divisions of DC and Uninterruptible AC Electrical Power Distribution and the associated instrumentation divisions are OPERABLE.

Leakage through the MSIVs is routed through the main steamline drain lines where large volumes and surface areas provide effective mechanisms to hold up and plate out the relatively low leakage flow. Leakage through the feedwater lines and from the PCCS condensers is addressed in Reference 2 subsection 15.4.4.5.2.

The RB HVAC system does not perform an ESF/safety-related function other than the isolation function of the CONAVS served area of the RB as described above. The RB is divided into clean and contaminated radiological zones. Under normal conditions, airflow is maintained from clean to potentially contaminated areas and then routed via the respective HVAC subsystem to the reactor building/fuel building stack. Under high radiation conditions, the contaminated areas (CONAVS) and refueling and pool area HVAC (REPAVS) served areas isolate to provide a hold up volume. Stack radiation monitors monitor RB effluents for radioactivity. If the radioactivity level rises above set levels, the discharge can be routed for treatment before further release.

The compartments within the RB are designed to withstand the maximum pressure due to a high-energy line break (HELB). Each line break analyzed is a double-ended break. In this analysis, the rupture producing the greatest blowdown of mass and enthalpy in conjunction with worst-case single active component failure is considered. Blowout panels between compartments provide flow paths to relieve pressure.

Personnel and equipment entrances to the RB consist of vestibules with interlocked doors and hatches. Large equipment access is by means of a dedicated, external access tower that provides the necessary interlocks. All openings through the RB boundary, such as personnel and equipment doors, are closed during normal operation and after a DBA by interlocks or administrative control. The doors are provided with position indicators and alarms, which are monitored in the control room.

BASES

APPLICABLE SAFETY ANALYSES	The radiological dose consequences for LOCAs are based on an assumed containment leak rate of 0.35 weight percent per day. The bulk of the primary containment leakage (0.34% per day) is released into the RB (CONAVS area) and leaks to the environment at a rate of 211 scfm (Ref. 2). Some credit is taken for hold up in the RB (CONAVS area) because the building is sealed during isolation. Reactor Building (CONAVS area) satisfies Criteria 3 of 10 CFR 50.36(c)(2)(ii).
LCO	This LCO requires that RB (CONAVS area) OPERABILITY is maintained by keeping all RB (CONAVS area) equipment hatches closed, keeping RB (CONAVS area) access doors closed, except for entry and exit, and ensuring RB CONAVS ventilation dampers actuate when required. RB (CONAVS area) OPERABILITY also requires RB (CONAVS area) leakage to be within limits. For each RB CONAVS isolation damper, the LCO requires OPERABILITY of the required safety-related initiators associated with DC and Uninterruptible AC Electrical Power Distribution Divisions required by LCO 3.8.6, "Distribution Systems - Operating."
APPLICABILITY	The RB (CONAVS area) is required to be OPERABLE in MODES 1, 2, 3, and 4 because a DBA could cause a release of radioactive material to containment and the RB (CONAVS area) provides an added barrier to fission product release from the containment during an accident. 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 RB (CONAVS area) is not required to be OPERABLE in MODES 5 and 6.
ACTIONS	The ACTIONS are modified by two Notes. The first Note allows the RB (CONAVS area) boundary to be unisolated intermittently under administrative controls. This Note only applies to openings in the RB (CONAVS area) 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

BASES

ACTIONS (continued)

openings, these controls consist of stationing a dedicated individual at the opening who is in continuous communication with control room operators. This individual will have a method to rapidly close the opening and to restore the boundary to a condition equivalent to the design condition when a need for RB (CONAVS area) isolation is indicated.

The second Note provides clarification that for the purpose of 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 RB (CONAVS area) boundary isolation damper. Complying with the Required Actions may allow for continued operation, and subsequent inoperable RB (CONAVS area) boundary isolation dampers are governed by subsequent Condition entry and application of associated Required Actions.

A.1 and A.2

In the event that there are one or more penetration flow paths with one RB (CONAVS area) boundary isolation damper inoperable, the affected penetration flow path(s) 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 damper, a closed manual damper, and a blind flange. For penetrations isolated in accordance with Required Action A.1, the device used to isolate the penetration should be the closest available device to the RB (CONAVS area). This Required Action must be completed within the 7-day Completion Time. The specified time period is reasonable considering the time required to isolate the penetration and the low probability of an accident that requires the boundary to be isolated occurring during this short time.

For affected penetrations that have been isolated in accordance with Required Action A.1, the affected penetration must be verified to be isolated on a periodic basis. This is necessary to ensure that RB (CONAVS area) penetrations required to be isolated following an accident, but no longer capable of being automatically isolated, will be in the isolation position should an event occur. This Required Action does not require any testing or device manipulation. Rather, it involves verification that the affected penetration remains isolated.

BASES

ACTIONS (continued)

B.1

With two RB (CONAVS area) boundary isolation dampers in one or more penetration flow paths inoperable, the affected penetration flow path must be isolated within 48 hours. 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 damper, a closed manual damper, and a blind flange. The 48-hour Completion Time is reasonable because of the low probability of an accident that requires the boundary to be isolated occurring during this short time.

C.1

If the RB (CONAVS area) is inoperable for reasons other than Condition A or B, the RB (CONAVS area) must be restored to OPERABLE within 24 hours. The 24-hour Completion Time provides a period of time to correct the problem that is commensurate with the importance of maintaining the RB (CONAVS area) boundary. This time period also ensures that the probability of an accident requiring RB (CONAVS area) OPERABILITY occurring during periods where the RB (CONAVS area) is inoperable is minimal.

D.1 and D.2

If the Required Action and associated Completion Time is 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 12 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 3.6.3.1.1

This SR requires periodic verification that all RB (CONAVS area) equipment hatches are closed. The 31-day Frequency is acceptable because RB (CONAVS area) equipment hatches are maintained in position under administrative controls that make a mis-positioned hatch unlikely.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.6.3.1.2

This SR requires periodic verification that one RB (CONAVS area) access door in each access opening is closed, except when open for entry and exit. The 31-day Frequency is acceptable because RB (CONAVS area) access doors are monitored and alarmed to prevent mis-positioning.

SR 3.6.3.1.3

This SR requires verification every 31 days of the continuity of the required safety-related initiators associated with DC and Uninterruptible AC Electrical Power Distribution Divisions required by LCO 3.8.6 for each RB (CONAVS area) boundary isolation damper.

The 31-day Frequency is acceptable because multiple initiators for each damper are capable of actuating the associated RB (CONAVS area) boundary isolation damper. Additionally, an alarm will provide prompt notification of loss of circuit continuity for the initiators.

This SR is modified by a Note that continuity is not required to be met for one required initiator circuit intermittently disarmed under administrative controls. This allows surveillance and maintenance with the assurance that the damper will not be inadvertently isolated. The operation of the disable/test switch in one division does not disable the RB (CONAVS area) boundary isolation damper because of the capability of the remaining required initiator(s).

SR 3.6.3.1.4

This SR requires periodic verification that RB (CONAVS area) ventilation dampers actuate on an actual or simulated isolation signal. The LOGIC SYSTEM FUNCTIONAL TESTs in LCO 3.3.6.2 and LCO 3.3.6.4 overlap this SR to provide complete testing of the safety function. The 24-month Frequency is based on engineering judgment and is acceptable based on the reliability of this type of component.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.6.3.1.5

This SR requires periodic verification that the RB (CONAVS area) exfiltration (leakage) rate is less than the limit, which is based on the assumptions in the radiological evaluations. Operating experience has shown that containment boundary designs similar to the RB (CONAVS area) boundary usually pass this Surveillance when performed at the 24-month Frequency. Therefore, the Frequency was concluded to be acceptable from a reliability standpoint.

REFERENCES

1. Chapter 6.
2. Chapter 15.

B 3.7 PLANT SYSTEMS

B 3.7.1 Isolation Condenser/Passive Containment Cooling System (IC/PCCS) Pools

BASES

BACKGROUND

The Ultimate Heat Sink (UHS) is the IC/PCCS Pools that transfer heat from the Isolation Condenser System (ICS) and the PCCS to the atmosphere (Ref. 1). The ICS removes heat from the Reactor Coolant System (RCS) following RCS isolation, a loss of feedwater or a Loss of Coolant Accident (LOCA). The PCCS removes heat from the containment following a LOCA or any transient that releases heat to the containment.

The IC/PCCS pools are located above and outside the containment boundary, directly above the drywell top slab. The condenser module associated with each ICS train and PCCS condenser is submerged in a separate subcompartment of the IC/PCCS pools. Subcompartments (i.e., pools) P3A, P3B, P3C, and P3D contain the condenser modules for the ICS trains. Subcompartments P4A, P4B, P4C, P4D, P4E, and P4F contain the condenser modules for the PCCS condensers.

Heat from the ICS and PCCS condensers is transferred to water in the associated subcompartment causing the water in the subcompartment to boil. Following reactor pressure vessel (RPV) isolation or a LOCA, subcompartment water temperature could rise to about 102°C (216°F). The steam formed will be non-radioactive and have a slight positive pressure. The steam from each subcompartment collects in the common air/steam space above the subcompartments and IC/PCCS pools. The steam is then released to the atmosphere through two large-diameter discharge vents located on opposite sides of the expansion pools. A moisture separator is installed at the entrance to the discharge vent lines to preclude excessive moisture carryover and loss of IC/PCCS pool water. No forced circulation equipment is required for operation (Refs. 2 and 3).

To support decay heat removal for 72 hours without operator action, water must be supplied to the ICS and PCCS subcompartments to replace the water lost by boiling. This water is supplied from the two IC/PCCS expansion pools, the equipment pool, and the reactor well pool.

Each ICS and PCCS subcompartment is connected to its associated expansion pool by a manually operated valve located below the water level, which allows makeup water from the expansion pool to flow into the bottom of the subcompartment. The subcompartment isolation valves are

BASES

BACKGROUND (continued)

normally locked open so that the full inventory of the associated expansion pool is available to any subcompartment. The subcompartment isolation valves can be closed to isolate a subcompartment allowing it to be emptied for maintenance of the condenser.

In addition to the ICS and PCCS subcompartments, each expansion pool is partitioned into three parts. Manually operated valves, which are normally locked open, separate each partition.

The equipment pool is connected to the reactor well pool through the reactor well gate, which is not installed during normal plant operation. By connecting the equipment pool and reactor well pool to the expansion pools, the volume of water available to the ICS and PCCS subcompartments is sufficient to support decay heat removal for 72 hours without operator action or the need to replenish the water in the expansion pools.

The equipment pool and reactor well pool are normally isolated from the expansion pools because the equipment pool and reactor well are maintained at a higher water level than the expansion pools. Each of the two expansion pools is connected to the equipment pool by two piping connections. One connection to each expansion pool is isolated by a squib-actuated cross-connect valve and the other connection is isolated by a fail-as-is double acting pneumatic piston cross-connect valve. Each connection also includes a manually operated valve, which is normally locked open. Opening one piping connection from the equipment pool to each expansion pool provides the required makeup from the equipment pool to the expansion pools.

The Safety System Logic and Control/Engineered Safety Features (SSLC/ESF) System controls the initiation signals and logic for the opening of the IC/PCCS expansion pool-to-equipment pool cross-connect valves. SSLC/ESF is a four division, separated protection logic system designed to provide a very high degree of assurance to both ensure initiation when required and prevent inadvertent initiation. The input and output trip determination is based upon a two-out-of-four logic arrangement. Each division of SSLC/ESF is configured such that all functions (e.g., the digital trip module (DTM) function and voter logic unit (VLU) function) are implemented in triply redundant processors to support the requirement that single divisional failures cannot result in inadvertent actuation.

BASES

BACKGROUND (continued)

Four separate instrument channels are used to monitor each IC/PCCS inner expansion pool level. Signals from sensors are multiplexed at the divisional level and the triply redundant sensor data is then transmitted to the SSLC/ESF triply redundant digital trip module (DTM) function for setpoint comparison. The output of each divisional DTM function (a trip/no-trip condition) is routed to all four divisional triply redundant VLU functions such that each divisional VLU function receives input from each of the four divisional DTM functions.

For maintenance purposes and added reliability, each DTM function has a division of sensors bypass such that all instruments in that division will be bypassed in the trip logic at the VLU functions. Thus, each VLU function will be making its trip decision on a two-out-of-three logic basis for each variable. It is possible for only one division of sensors bypass condition to be in effect at any time.

The processed trip signal from its own division and trip signals from the other three divisions are processed in the triply redundant VLU function for two-out-of-four voting. Each pair of IC/PCCS expansion pool-to-equipment pool cross-connect valves receive an open signal on low level in the associated inner expansion pool.

Each expansion pool-to-equipment pool cross-connect squib valve is equipped with four squib initiators. Each expansion pool-to-equipment pool cross-connect pneumatic valve is equipped with four solenoid valves (i.e., initiators). A signal to any of the four initiators will actuate the associated cross-connect valve. Three of the four initiators on each valve are actuated by SSLC/ESF. As such, at least two of the three safety-related initiators on each valve will be associated with divisions required by LCO 3.8.6, "Distribution Systems - Operating." The fourth initiator is actuated by the Diverse Protection System (DPS), which is designed to mitigate digital protection system common mode failures.

Cooling and clean up of IC/PCCS pool water is performed by Fuel and Auxiliary Pools Cooling System (FAPCS). The FAPCS includes a separate subsystem with its own pump, heat exchanger, and water treatment unit that is dedicated for cooling and cleaning of the IC/PCCS pools to prevent radioactive contamination of the IC/PCCS pools. The FAPCS includes flow paths for post-accident make-up water transfer, from the fire protection system and off-site water supply sources to the IC/PCCS pools (Ref. 1).

BASES

APPLICABLE SAFETY ANALYSES	In the event of a LOCA, the passive PCCS is required to maintain the containment peak pressure and temperature below design limits for at least 72 hours after the LOCA without operator action (Ref. 3). In the event of reactor isolation or a station blackout, the ICS must maintain the reactor coolant system pressure and temperature below design limits and remove core decay heat for at least 72 hours after reactor isolation without operator action (Ref. 2). The IC/PCCS pools are also needed as a heat sink for the ICS condensers when ICS is used as a backup to the Reactor Water Cleanup/Shutdown Cooling (RWCU/SDC) System for decay heat removal when shutdown. The IC/PCCS pools satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).
LCO	This LCO requires that the IC/PCCS pools are OPERABLE. Operability requires the IC/PCCS pools be maintained within specified limits for minimum level and maximum average temperature. To ensure that the total volume of water in the IC/PCCS pools is available to the ICS and PCCS condensers, manual isolation valves between the partitions within each expansion pool and between the equipment pool and each expansion pool must be locked open. Cross-connect valves between the equipment pool and the expansion pools must open automatically on a low water level signal from the associated expansion pool. Additionally, the reactor well gate, which connects the reactor well to the equipment pool, must be removed. OPERABILITY of the expansion pool-to-equipment pool cross-connect function requires OPERABILITY of three channels of safety-related IC/PCCS expansion pool level instrumentation in each pool and three safety-related actuation logic divisions. OPERABILITY of an instrumentation channel requires OPERABILITY of the instrumentation from the input variable sensor through the DTM function. Each instrumentation channel must have its setpoint in accordance with Specification 5.5.11, “Setpoint Control Program (SCP).” OPERABILITY of an actuation logic division requires OPERABILITY of the circuitry from the output of the DTM function through the VLU function, the timers, and the load drivers.

BASES

LCO (continued)

OPERABILITY of each expansion pool-to-equipment pool squib cross-connect valve and pneumatic cross-connect valve requires OPERABILITY of the DPS initiator and two safety-related initiators.

The required safety-related channels, divisions, and initiators are those associated with the DC and Uninterruptible AC Electrical Power Distribution Divisions required by LCO 3.8.6, "Distribution Systems - Operating."

OPERABILITY of the instrumentation and actuation logic associated with the DPS initiators is addressed by LCO 3.3.8.1, “Diverse Protection System (DPS).”

APPLICABILITY

The IC/PCCS pools are required to be OPERABLE in MODES 1, 2, 3, and 4 because the PCCS and ICS could be required to respond to an event that caused pressurization and heat up of containment or the ICS could be required to respond to an RPV isolation.

Requirements for the IC/PCCS expansion pools in MODE 5 are determined by the requirements of LCO 3.5.5, "Isolation Condenser System (ICS) - Shutdown."

ACTIONS

A.1

This Condition applies when one or both expansion pools have one equipment pool cross-connect valve DPS initiator inoperable. In this Condition, required safety-related initiators will actuate the expansion pool-to-equipment pool cross-connect valves needed to support decay heat removal for 72 hours without operator action concurrent with any additional single failure, including digital protection system common mode failures.

In this Condition, the inoperable expansion pool-to-equipment pool DPS initiators must be restored to OPERABLE status the next time the plant is placed in MODE 5 (i.e., prior to entering MODE 2 or MODE 4 from MODE 5). This Completion Time is acceptable because the remaining DPS initiator and the required safety-related initiators will actuate the minimum number of expansion pool-to-equipment pool cross-connect valves required to support decay heat removal for 72 hours concurrent with any additional single failure.

BASES

ACTIONS (continued)

B.1

This Condition applies when one or both expansion pools have both equipment pool cross-connect valve DPS initiators inoperable. In this Condition, required safety-related initiators will actuate the minimum expansion pool-to-equipment pool cross-connect valves assumed in the design basis analysis concurrent with any additional single failure. However, design features intended to mitigate the possibility of digital protection system common mode failures are not available.

In this Condition, at least one DPS initiator in each affected expansion pool must be restored to OPERABLE status within 30 days. This Completion Time is acceptable because the required safety-related initiators will actuate the minimum number of expansion pool-to-equipment pool cross-connect valves required to support decay heat removal for 72 hours without operator action concurrent with any additional single failure.

C.1

This Condition applies when one or both IC/PCCS expansion pools have one equipment pool connection line inoperable for reasons other than Condition A. In this Condition, failure of an additional expansion pool-to-equipment pool connection line could result in the need for operator action to re-fill the IC/PCCS pool in less than 72 hours following any event that requires either PCCS or ICS for decay heat removal.

In this Condition, the expansion pool-to-equipment pool connection line(s) must be restored to OPERABLE status within 30 days. This Completion Time is acceptable based on engineering judgment considering that substantial decay heat removal capacity would remain available even if an additional expansion pool-to-equipment pool connection line failed and the low probability of a failure of an additional expansion pool-to-equipment pool connection line failure in conjunction with an event that requires either PCCS or ICS for decay heat removal.

D.1

With one required IC/PCCS expansion pool level instrumentation channel inoperable, the affected required channel must be restored to OPERABLE status within 20 hours. In this Condition, actuation trip capability is maintained but a single failure cannot be accommodated.

BASES

ACTIONS (continued)

The 20-hour Completion Time is acceptable based on engineering judgment considering the redundancy of the instrumentation design and the low probability of an event requiring actuation of the expansion pool-to-equipment pool cross-connect during this period.

Alternatively, if the instrumentation channel cannot be restored to OPERABLE status, Condition G must be entered and its Required Action taken when the Completion Time of Required Action D.1 expires.

It should be noted that if more than one required instrumentation channel is inoperable, then the cross-connect may not actuate as required; therefore, the IC/PCCS Pools must be declared inoperable and Condition F must be entered.

<u>E.1</u>

Condition E exists when one required IC/PCCS expansion pool-to-equipment pool cross-connect actuation division is inoperable. In this Condition, actuation trip capability is maintained but a single failure cannot be accommodated. The 20-hour Completion Time is acceptable based on engineering judgment considering the redundancy of the actuation design and the low probability of an event requiring cross-connect actuation during this period.

Alternatively, if the actuation division cannot be restored to OPERABLE status, Condition G must be entered and its Required Action taken when the Completion Time of Required Action E.1 expires.

It should be noted that if more than one required actuation division is inoperable, then the cross-connect may not actuate as required; therefore, the IC/PCCS Pools must be declared inoperable and Condition F must be entered.

<u>F.1</u>

If the IC/PCCS pool is inoperable for reasons other than Condition A, B, C, D, or E, then the ICS and PCCS may not be capable of performing their required safety function and the initial conditions used in the analyses in References 2 and 3 may not be met. Required Action F.1 requires that the IC/PCCS pools be restored within 8 hours. The Completion Time of 8 hours is acceptable based on the remaining heat removal capability of the IC/PCCS pools and the alternate methods for providing makeup to the IC/PCCS pools.

BASES

ACTIONS (continued)

G.1 and G.2

If the Required Action and associated Completion Time of Condition A, B, C, D, E, or F is not met, 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 12 hours and to MODE 5 within 36 hours. The Completion Times are reasonable, based on plant design, to reach required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.7.1.1

Performance of the CHANNEL CHECK once every 12 hours ensures that a gross failure of the IC/PCCS expansion pool level instrumentation has not occurred.

The SSLC/ESF is cyclically tested from the sensor input point to the logic contact output by online self-diagnostics. The self-diagnostic capabilities include microprocessor checks, system initialization, watchdog timers, memory integrity checks, input/output (I/O) data integrity checks, communication bus interface checks, and checks on the application program (checksum).

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 match criteria, it may be an indication that the instrument has drifted outside its limit.

The Surveillance Frequency is based upon operating experience that demonstrates channel failure is rare. The CHANNEL CHECK every 12 hours supplements less formal, but more frequent checks of channels during normal operational use of the displays associated with the channels required by the LCO.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.7.1.2 and SR 3.7.1.3

This SR requires verification every 24 hours that the water levels in each expansion pool and the water level in the equipment pool or reactor well are within specified limits. These levels are necessary to ensure that the volume of water in the IC/PCCS pools is sufficient to support decay heat removal via the ICS and/or the PCCS for 72 hours without the need to replenish the water in the expansion pools. The 24 hour frequency is acceptable because abnormal water levels are identified by alarms and indication in the control room.

SR 3.7.1.3 is modified by a Note that specifies that this SR is not required to be met in MODES 3 and 4. Considering the reduced decay heat loads following events initiated after the reactor is shut down, isolation of these pools from the IC/PCCS expansion pools when in Modes 3 and 4 will not result in a significant reduction in the 72 hours assumed available to provide makeup to the IC/PCCS pools.

SR 3.7.1.4

This SR requires verification every 24 hours that the bulk average temperature of the available IC/PCCS pools is ≤ 43.3°C (110°F). The bulk average temperature is calculated based on the volume and temperature of the water in the expansion pools, the connected ICS and PCCS subcompartments (isolated subcompartments are addressed in LCO 3.5.4, "Isolation Condenser System (ICS) - Operating" and LCO 3.6.1.7, "Passive Containment Cooling System (PCCS)," respectively), the equipment pool, and the reactor well. The water volume in any isolated subcompartments, or the equipment pool when inoperabilities render it unavailable, are not averaged to meet the requirements of SR 3.7.1.4. This value for the average temperature of the IC/PCCS pools is an assumption in the analyses described in References 2 and 3 that determined that the heat sink capacity of the IC/PCCS pools is sufficient to support decay heat removal for 72 hours without the need to replenish the water in the expansion pools. The 24-hour frequency is acceptable because operators will be promptly alerted to abnormal water temperatures by alarms and indication in the control room.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.7.1.5

This SR requires periodic verification that the supply pressure to the expansion pool-to-equipment pool pneumatic cross-connect valve accumulators (i.e., Instrument Air System (IAS)) is greater than or equal to the specified limit. An accumulator on each expansion pool-to-equipment pool pneumatic cross-connect valve provides pneumatic pressure for valve actuation. The 31-day Frequency is acceptable because IAS low-pressure alarms provide prompt notification of an abnormal pressure in the IAS.

SR 3.7.1.6

This SR requires a periodic verification of the continuity of the DPS initiator and two safety-related initiators associated with DC and Uninterruptible AC Electrical Power Distribution Divisions required by LCO 3.8.6, "Distribution Systems - Operating," for each expansion pool-to-equipment pool cross-connect valve.

The 31-day Frequency is acceptable because either of the expansion pool-to-equipment pool lines for each expansion pool is capable of performing the required function. Additionally, an alarm will provide prompt notification of loss of circuit continuity for the required initiators in each expansion pool-to-equipment pool cross-connect valve.

This SR is modified by a Note that continuity is not required to be met for one required initiator intermittently disabled under administrative controls. This allows the continuity monitor to be tested and allows surveillance and maintenance with the assurance that the valve will not be opened inadvertently.

SR 3.7.1.7

A CHANNEL FUNCTIONAL TEST is performed on each required IC/PCCS expansion pool level instrumentation channel to ensure the entire channel will perform the intended function. This test ensures a complete CHANNEL FUNCTIONAL TEST of required instrument channels from the sensor input through the DTM function.

SURVEILLANCE REQUIREMENTS (continued)

The SSLC/ESF is cyclically tested from the sensor input point to the logic contact output by online self-diagnostics. The self-diagnostic capabilities include microprocessor checks, system initialization, watchdog timers, memory integrity checks, input/output (I/O) data integrity checks, communication bus interface checks, and checks on the application program (checksum).

The Frequency of 31 days is based on the reliability of the instrumentation channels.

SR 3.7.1.8

This SR requires verification every 24 months that the manual isolation valve on each expansion pool-to-equipment pool line and between each IC/PCCS expansion pool partition is locked open. This SR is needed to ensure that the full volume of water in each expansion pool is available to the ICS and PCCS subcompartments. If this SR is not met, the ICS and PCCS may not be capable of performing their design functions. The 24-month Frequency for this SR is based on engineering judgment and is acceptable because the manual isolation valves between the IC/PCCS pool partitions are locked open and maintained in their correct position under administrative controls.

SR 3.7.1.9

This SR requires verification every 24 months that the reactor well-to-equipment pool gate is not installed. This SR is necessary to ensure that the volume of water in the reactor well is available to the ICS and/or the PCCS condensers. The volume of water in the reactor well is needed to support decay heat removal for 72 hours without the need to replenish the water in the expansion pools. The 24-month frequency is acceptable because installation of the reactor well-to-equipment pool gate is a significant change in plant status that would not occur without the cognizance of the operators.

This SR is modified by a Note that specifies that this SR is not required to be met in MODES 3 and 4. Considering the reduced decay heat loads following events initiated after the reactor is shutdown, isolation of this pool from the IC/PCCS expansion pools when in Modes 3 and 4 will not result in a significant reduction in the 72 hours assumed available to provide makeup to the IC/PCCS pools.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.7.1.10

This SR requires verification every 24 months that each cross-connect valve between the IC/PCCS expansion pools and the equipment pool actuates on an actual or simulated automatic initiation signal. At least one of the two cross-connect valves that isolate each expansion pool from the equipment pool must be open to ensure that the volume of water in the equipment pool and the reactor well is available to the ICS and/or the PCCS condenser. The volume of water in the reactor well and the equipment pool is needed to support decay heat removal for 72 hours without the need to replenish the water in the expansion pools. The LOGIC SYSTEM FUNCTIONAL TEST in SR 3.7.1.12 and LCO 3.3.8.1 overlap this SR to provide complete testing of the assumed safety function.

This 24-month Frequency is consistent with the normal refueling interval. This interval will allow the SR to be performed during a plant outage. This SR is modified by a Note that excludes valve actuation as a requirement for this SR to be met. This is acceptable because the valves are subject to the Inservice Test Program.

This SR is modified by a Note that specifies that this SR not required to be met in MODES 3 and 4. Considering the reduced decay heat loads following events initiated after the reactor is shutdown, isolation of this pool from the IC/PCCS expansion pools when in Modes 3 and 4 will not result in a significant reduction in the 72 hours assumed available to provide makeup to the IC/PCCS pools.

SR 3.7.1.11

This SR requires a CHANNEL CALIBRATION of IC/PCCS expansion pool level instrumentation channels that actuate the expansion pool-to-equipment pool squib cross-connect valves and pneumatic cross-connect valves. CHANNEL CALIBRATION is a complete check of the instrument loop and the sensor. This test verifies that the channel responds to the measured parameters within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to the required nominal trip setpoint within the "as-left tolerance" to account for instrument drifts between successive calibrations consistent with the methods and assumptions required by the Setpoint Control Program. The Frequency is based upon the assumption of a 24-month calibration interval in the determination of the magnitude of equipment drift in the setpoint analysis.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.7.1.12

This SR requires performance of a LOGIC SYSTEM FUNCTIONAL TEST for the logic associated with automatic opening of the IC/PCCS expansion pool-to-equipment pool cross-connect valves. The LOGIC SYSTEM FUNCTIONAL TEST demonstrates the OPERABILITY of the required logic for a specific division.

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 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 24-month Frequency.

SR 3.7.1.13

This SR requires verification that each ICS and PCCS pool subcompartment has an unobstructed path for steam release through moisture separator to the atmosphere. This SR is needed to ensure that steam formed in the ICS and PCCS subcompartments will be properly vented to the atmosphere. The Frequency of 48 months on a STAGGERED TEST BASIS for the flow path associated with each moisture separator is based on engineering judgment and the simplicity of the design. This Frequency is acceptable because the flow path from the ICS subcompartments to the expansions pool area and through the moisture separators will be verified whenever the ICS is used.

REFERENCES

1. Chapter 9.
2. Chapter 5.
3. Chapter 6.

B 3.7 PLANT SYSTEMS

B 3.7.2 Control Room Habitability Area (CRHA) Heating, Ventilation, and Air Conditioning (HVAC) Subsystem (CRHAVS)

BASES

BACKGROUND

The CRHAVS trains, the CRHA boundary, and the CRHA heat sinks provide a protected environment from which occupants can control the unit following an uncontrolled release of radioactivity[, hazardous chemicals,] or smoke.

COL 16.0-1-A 3.7.2-1

The CRHAVS includes two independent and redundant CRHAVS trains that provide pressurization and radiologically filtered air to maintain control room habitability during a radiological emergency or loss of preferred power. Each CRHA train each includes: one 100% capacity Emergency Filtration Unit (EFU); two 100% capacity safety-related EFU fans in parallel; and four electrically operated, normally closed discharge EFU isolation dampers, which are mounted in a parallel configuration of two dampers in series. Each EFU fan and an associated set of dampers in series are powered from the same electrical division. Failure of one EFU fan or the associated set of dampers does not affect the operation of the other set in the same CRHA train. If flow detectors installed in the EFU discharge duct detect low flow, the operating fan motor is de-energized, its electrically operated discharge dampers are closed, a stand-by (second in the unit) fan motor is energized and its electrically operated discharge dampers are opened. If the discharge flow is not sufficiently improved or if radiation is detected downstream of the EFU, the affected CRHAVS train is automatically disengaged and the second train is energized, following the protocol described above. Each EFU consists of a medium efficiency filter, a high efficiency particulate air (HEPA) filter, a carbon adsorption filter, and a post-filter downstream of the carbon filter. The EFUs are maintained in accordance with Specification 5.5.13, “Ventilation Filter Testing Program.”

The CRHA boundary confines the spaces that control room occupants inhabit to control the unit during normal and accident conditions. The CRHA boundary is the combination of walls, floor, roof, ducting, doors, penetrations, and equipment that physically form the CRHA. The CRHA boundary includes safety-related, air operated isolation dampers connected in series, which isolate the control room main air ventilation duct, the smoke purge intake duct, the smoke purge exhaust duct, and the restroom exhaust duct. Because the air-operated dampers in each

BASES

BACKGROUND (continued)

redundant pair are in series, either damper can close the airflow path. Each set of dampers is controlled by four independent solenoids, which ensures that the safety-related function of the system can be performed with the loss of any two divisions of power.

The CRHA boundary is maintained in accordance with Specification 5.5.12, “Control Room Habitability Area (CRHA) Boundary Program,” to ensure that the inleakage of unfiltered air into the CRHA will not exceed the inleakage assumed in the licensing basis analysis of design basis accident (DBA) consequences to CRHA occupants.

The CRHA heat sinks maintain CRHA temperature following loss of normal CRHA cooling because the CRHA heat loads are passively dissipated to the heat sinks. The CRHA heat sinks consist of three groups: the CRHA (i.e., the CRHA walls, floor, ceiling, interior walls), adjacent corridors, and HVAC chases; adjacent Q-DCIS and N-DCIS equipment rooms and electrical chases; and, adjacent HVAC equipment rooms and safety portions of the CRHA rooms. When the temperature of each CRHA heat sink is maintained within the specified limit, the CRHA heat sinks are sufficient to limit the CRHA temperature to 33.9°C (93°F).

CRHA Recirculation air-handling units (AHUs) provide normal cooling to the CRHA whenever offsite or onsite AC power is available. During the first two hours after a loss of preferred power (LOPP), the recirculation AHU fans and associated auxiliary cooling units are powered from a nonsafety-related battery. If an ancillary diesel generator is available, power for a recirculation AHU fan and auxiliary cooling unit can be provided indefinitely during a CRHA isolation event that includes a LOPP. However, if the Recirculation AHUs are not available during the LOPP, safety-related temperature sensors with two-out-of-four logic automatically trip the power to selected N-DCIS components in the MCR to reduce the N-DCIS heat load.

CRHAVS trains are actuated by the Safety System Logic and Control System/Engineered Safety Features (SSLC/ESF) described in the Bases for LCO 3.3.7.1, " Control Room Habitability Area (CRHA) Heating, Ventilation, and Air Conditioning (HVAC) Subsystem (CRHAVS) Instrumentation" and LCO 3.3.7.2, " Control Room Habitability Area (CRHA) Heating, Ventilation, and Air Conditioning (HVAC) Subsystem (CRHAVS) Actuation." An actuation signal starts one EFU fan in the EFU

BASES

BACKGROUND (continued)

train that is designated as the primary, opens the associated EFU isolation dampers, closes the normal air supply duct and restroom exhaust safety-related isolation dampers, and stops the nonsafety-related normal air supply fans. Power to each of the four EFU fans (two in each CRHA train) and associated dampers and the four initiators for each pair of CRHA boundary dampers is supplied from a different division of the DC and Uninterruptible AC Electrical Power Distribution. As such, no single active component failure will prevent automatic initiation and successful operation of the minimum required CRHAVS components when any three of the four divisions of DC and Uninterruptible AC Electrical Power Distribution and the associated instrumentation divisions are OPERABLE.

The CRHAVS is designed to maintain a habitable environment in the CRHA for 72 hours continuous occupancy after a design basis accident (DBA) concurrent with a loss of all onsite and offsite AC power and, upon recovery of onsite or offsite AC power, for an additional 27 days continuous occupancy, without exceeding 0.05 Sv (5 rem) total effective dose equivalent (TEDE). Controls to manually isolate the CRHA and to manually actuate CRHAVS following indication of a radiological event (indicative of conditions that could result in radiation exposure to CRHA occupants) are provided. CRHAVS operation in maintaining CRHA habitability is discussed in Section 6.4 and Section 9.4.1 (Refs. 1 and 2, respectively).

APPLICABLE SAFETY ANALYSES

The ability of the CRHAVS to maintain the habitability of the CRHA is an explicit assumption for the safety analyses presented in Chapter 6 and Chapter 15, (Refs. 1 and 3, respectively). The isolation mode of the CRHAVS is assumed to operate following a DBA. The radiological dose to CRHA occupants as a result of various DBAs is summarized in Reference 3. No single active failure will cause the loss of outside air to the CRHA. The CRHAVS provides protection from smoke [and hazardous chemicals] to the CRHA occupants. [The analysis of hazardous chemical releases demonstrates that the toxicity limits are not
COL 16.0-1-A 3.7.2-1 exceeded in the CRHA following a hazardous chemical release (Ref. 1).] The evaluation of a smoke challenge demonstrates that it will not result in the inability of the CRHA occupants to control the reactor either from the main control room or from the remote shutdown panels (Ref. 2).

CRHA heat sinks in the CRHA and adjacent spaces must be maintained consistent with the assumptions in Reference 2 to ensure that the CRHA temperature can be maintained for 72 hours following an event that includes loss of CRHAVS cooling.

BASES

APPLICABLE SAFETY ANALYSES (continued)

The CRHAVS satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

OPERABILITY of the CRHAVS requires: OPERABILITY of two redundant one hundred percent capacity trains of the CRHAVS; OPERABILITY of the CRHA boundary; and OPERABILITY of the CRHA heat sinks.

Each CRHAVS train is OPERABLE when:

a. One EFU fan and the two associated EFU isolation dampers are OPERABLE and associated with a DC and Uninterruptible AC Electrical Power Distribution Division required by LCO 3.8.6, "Distribution Systems – Operating," and LCO 3.8.7, "Distribution Systems – Shutdown,"

b. The EFU HEPA filter and carbon adsorber are not excessively restricting flow and are capable of performing their filtration functions, and

c. Both EFU fan backdraft dampers are OPERABLE.

The standby EFU fan and associated EFU isolation dampers in each CRHAVS train are not required for CRHAVS train OPERABILITY.

The CRHA boundary is OPERABLE when:

a. CRHA boundary is maintained in accordance with Specification 5.5.12, “Control Room Habitability Area (CRHA) Boundary Program,”

b. The CRHA boundary isolation dampers (excluding the EFU isolation dampers associated with the EFU trains) are OPERABLE or one of the dampers in the flow path is closed, and

c. The CRHA boundary isolation dampers associated with the EFU trains are closed when the associated EFU fans are not running.

The CRHA heat sinks are OPERABLE when the CRHA and adjacent spaces are maintained within the limits in SR 3.7.2.1 to ensure that the CRHA temperature can be maintained for 72 hours following an event that includes loss of CRHAVS cooling.

BASES

LCO (continued)

The LCO is modified by a Note allowing the CRHA boundary to be opened intermittently under administrative controls. This Note only applies to openings in the CRHA 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 consist of stationing a dedicated individual at the opening who is in continuous communication with the operators in the CRHA. This individual will have a method to rapidly close the opening and to restore the CRHA boundary to a condition equivalent to the design condition when a need for CRHA isolation is indicated.

APPLICABILITY

In MODES 1, 2, 3, and 4, the CRHAVS must be OPERABLE to ensure that the CRHA will remain habitable during and following a DBA, since the DBA could lead to a fission product release.

In MODES 5 and 6, the probability and consequences of a DBA are reduced due to the pressure and temperature limitations in these MODES. Therefore, maintaining the CRHAVS OPERABLE is not required in MODES 5 or 6, except during operations with a potential for draining the reactor vessel (OPDRVs), which is a situation under which significant radioactive releases can be postulated.

ACTIONS

A.1 and A.2

Condition A represents a potential for degradation of the CRHA passive heat sink. The ACTIONS provide a tiered response that focuses on returning the affected heat sink area average air temperature(s) to within the established design limit and restoring the CRHA passive heat sink to OPERABLE status in a reasonable time period. When the average temperature of one or more CRHA heat sink(s) is greater than the limit specified in SR 3.7.2.1, Required Action A.1 requires that the average air temperature of each CRHA heat sink be restored to within the limit within 8 hours. The 8-hour Completion Time is acceptable based on engineering judgment to evaluate and repair any discovered inoperabilities or provide an alternate means of cooling the affected CRHA heat sink area to restore CRHA heat sink average air temperatures to within limits.

ACTIONS (continued)

Required Action A.2 requires that the average temperature of each CRHA heat sink be restored to within limits within 24 hours. The 24-hour Completion Time is acceptable based on engineering judgment to determine that the affected CRHA heat sink structural materials temperatures are within limits.

Restoration of the CRHA heat sinks is verified by administrative evaluation considering the length of time and extent of the CRHA heat sink average air temperature excursion outside of limits, or by direct measurement of the CRHA heat sink area structural materials temperatures.

While in this Condition, the unit is more vulnerable to a trip of selected N-DCIS components in the MCR. It is, therefore, appropriate that the unit operators' attention be focused on minimizing the potential impact of a loss of selected N-DCIS components by stabilizing the unit and restoring the affected heat sink area temperatures to within limits. In addition to limiting the degradation of the CRHA heat sink and restoring temperatures to within limits, the Completion Times of Required Actions A.1 and A.2 minimize the risk associated with the potential for loss of selected N-DCIS components during a plant transient associated with a required shutdown.

B.1, B.2, and B.3

COL 16.0-1-A 3.7.2-1

If the unfiltered inleakage of potentially contaminated air past the CRHA boundary can result in CRHA occupant radiological dose greater than the calculated dose of the licensing basis analyses of DBA consequences (allowed to be up to 5 rem TEDE), or inadequate protection of CRHA occupants from [hazardous chemicals or] smoke, the CRHA boundary is inoperable. The CRHA boundary must be restored to OPERABLE status within 90 days.

COL 16.0-1-A 3.7.2-1

During the period that the CRHA boundary is considered inoperable, action must be initiated immediately to implement mitigating actions to lessen the effect on CRHA occupants from the potential hazards of a radiological [or chemical] event or a challenge from smoke. Actions must be taken within 24 hours to verify that in the event of a DBA, the mitigating actions will ensure that CRHA occupant radiological exposures will not exceed the calculated dose of the licensing basis analyses of DBA consequences, and that CRHA occupants are protected from [hazardous chemicals and] smoke. These mitigating actions (i.e., actions that are

BASES

ACTIONS (continued)

taken to offset the consequences of the inoperable CRHA 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 90 day Completion Time is reasonable based on the determination that the mitigating actions will ensure protection of CRHA occupants within analyzed limits while limiting the probability that CRHA occupants will have to implement protective measures that may 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 90 day Completion Time is a reasonable time to diagnose, plan and possibly repair, and test most problems with the CRHA boundary.

C.1

With one CRHAVS train inoperable for reasons other than Condition A or B, the inoperable CRHAVS train must be restored to OPERABLE status within 7 days. In this Condition, the remaining OPERABLE CRHAVS train is adequate to perform the CRHA occupant protection function. However, the overall reliability is reduced because a failure in the OPERABLE train could result in loss of CRHAVS function. The 7-day Completion Time is based on engineering judgment considering the low probability of a DBA occurring during this time period and that the remaining train can provide the required capabilities.

D.1 and D.2

If the Required Action and associated Completion Time of Condition A, B, or C are not met when in MODE 1, 2, 3, or 4 or if two CRHAVS trains are inoperable when in MODE 1, 2, 3, or 4 for reasons other than Condition A or B, the unit must be placed in a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 12 hours and to MODE 5 within 36 hours. The Completion Time is reasonable, based on plant design, to reach required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

BASES

ACTIONS (continued)

E.1

If the Required Action and associated Completion Time of Condition A or B are not met during OPDRVs or if two CRHAVS trains are inoperable during OPDRVs, action must be taken to immediately suspend activities that represent a potential for releasing radioactivity that might require isolation of the CRHA. This places the unit in a condition that minimizes risk.

Applicable actions must be initiated immediately to suspend OPDRVs to minimize the probability of a vessel draindown and subsequent potential for fission product release. Actions must continue until the OPDRVs are suspended.

F.1 and F.2

If the Required Action and associated Completion Time of Condition C are not met during OPDRVs (i.e., the inoperable CRHAVS train cannot be restored to OPERABLE status), the OPERABLE CRHAVS train may be placed in the isolation mode. This action ensures that the remaining train is OPERABLE, that no failures that would prevent automatic actuation will occur, and that any active failure will be readily detected.

An alternative to Required Action F.1 is to immediately suspend activities that present a potential for releasing radioactivity that might require isolation of the CRHA. This places the unit in a condition that minimizes risk. Applicable actions must be initiated immediately to suspend OPDRVs to minimize the probability of a vessel draindown and subsequent potential for fission product release. Actions must continue until the OPDRVs are suspended.

SURVEILLANCE REQUIREMENTS

SR 3.7.2.1

This SR verifies every 24 hours that the average temperature for each CRHA heat sink is within established design limits (Ref. 4). The CRHA heat sinks and associated design limits for initial temperature are as shown in Table B 3.7.2-1. The CRHA heat sinks consist of three groups: the CRHA (i.e., the CRHA walls, floor, ceiling, interior walls), adjacent corridors, and HVAC chases; adjacent Q-DCIS and N-DCIS equipment rooms and electrical chases; and, adjacent HVAC equipment rooms and safety portions of the CRHA rooms. A CRHA heat sink temperature is assumed to be within the specified limit if the average of the air

BASES

SURVEILLANCE REQUIREMENTS (continued)

temperature in the heat sink has been within the specified limit since the last performance of the surveillance. This is acceptable because the temperature change of the CRHAVS heat sink area structural materials will lag behind the temperature change of the CRHA heat sink area average air temperature with respect to increasing temperature. Therefore, CRHA heat sink area average air temperature outside of the specified limit provides a conservative indication of a potential degradation of the CRHA heat sink. In addition, the CRHA heat up calculation assumes that the CRHA heat sink area structural materials are in equilibrium with the CRHA heat sink area average air temperature.

The surveillance limit for each of the CRHA heat sinks is equal to or more conservative than the initial temperature assumed in the CRHA thermal analysis. This SR ensures that the nonsafety-related recirculation AHUs are performing as required to maintain initial CRHA heat sink temperatures consistent with the assumptions in the safety analysis, which will ensure that the CRHA temperature will not exceed the required conditions after loss of CRHAVS cooling.

The 24 hour Frequency is acceptable based on the availability of temperature indication in the main control room and the slow change in the actual heat sink temperature following a change in the air temperature being monitored.

SR 3.7.2.2

This SR verifies that a CRHAVS train in a standby mode starts on demand and continues to operate. Standby systems should be checked periodically to ensure that they start and function properly. As the environmental and normal operating conditions of this system are not severe, testing each train once every month provides an adequate check on this system. Systems without heaters need only be operated for ≥ 15 minutes to demonstrate the function of the system. Furthermore, the 31 day Frequency is based on the known reliability of the equipment and the two train redundancy available.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.7.2.3

This SR verifies that the required CRHAVS testing is performed in accordance with the Ventilation Filter Testing Program (VFTP). 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 3.7.2.4

This SR verifies that each CRHA isolation damper closes and each CRHAVS train starts and operates on an actual or simulated initiation signal. The LOGIC SYSTEM FUNCTIONAL TEST in LCO 3.3.7.2, “Control Room Habitability Area (CRHA) Heating, Ventilation, and Air Conditioning (HVAC) Subsystem (CRHAVS) Actuation,” overlaps this SR to provide complete testing of the safety function.

The 24 month Frequency is based on the normal refueling frequency, and is consistent with the Frequency of the surveillances performed for the actuation instrumentation.

SR 3.7.2.5

This SR verifies that selected main control room N-DCIS electrical loads automatically de-energize on an actual or simulated initiation signal. Temperature sensors with two-out-of-four logic automatically trip the power to selected N-DCIS components in the main control room (MCR) to reduce the heat load if the AHUs are not powered.

The LOGIC SYSTEM FUNCTIONAL TEST in LCO 3.3.7.2 overlaps this SR to provide complete testing of the safety function. The 24 month Frequency is based on the normal refueling frequency, and is consistent with the Frequency of the surveillances performed for the actuation instrumentation.

SR 3.7.2.6

This SR requires a CHANNEL CALIBRATION of the main control room temperature instrumentation channels that automatically trip the power to N-DCIS components in the main control room (MCR) to reduce the heat load if the AHUs are not powered. CHANNEL CALIBRATION is a

BASES

SURVEILLANCE REQUIREMENTS (continued)

complete check of the instrument loop and the sensor. This test verifies that the channel responds to the measured parameters within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to the required nominal trip setpoint within the "as-left tolerance" to account for instrument drifts between successive calibrations consistent with the methods and assumptions required by the Setpoint Control Program. The Frequency is based upon the assumption of a 24-month calibration interval in the determination of the magnitude of equipment drift in the setpoint analysis.

SR 3.7.2.7

COL 16.0-1-A 3.7.2-1

This SR verifies the OPERABILITY of the CRHA boundary by testing for unfiltered air inleakage past the CRHA boundary and into the CRHA. The details of the testing are specified in the Control Room Habitability Area (CRHA) Boundary Program. The CRHA is considered habitable when the radiological dose to CRHA occupants calculated in the licensing basis analyses of DBA consequences is no more than 5 rem TEDE and the CRHA occupants are protected from [hazardous chemicals and] smoke. This SR verifies that the unfiltered air inleakage into the CRHA 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 CRHA boundary to OPERABLE status provided mitigating actions can ensure that the CRHA remains within the licensing basis habitability limits for the occupants following an accident. Compensatory measures are discussed in Regulatory Guide 1.196, Section C.2.7.3, (Ref. 5) which endorses, with exceptions, NEI 99-03, Section 8.4 and Appendix F (Ref. 6). 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 (Ref. 7). Options for restoring the CRHA boundary to OPERABLE status include changing the licensing basis DBA consequence analysis, repairing the CRHA 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 CRHA boundary has been restored to OPERABLE status.

BASES

REFERENCES

1. Section 6.4.
2. Section 9.4.1.
3. Section 15.4.
4. Section 3H.
5. Regulatory Guide 1.196.
6. NEI 99-03, "Control Room Habitability Assessment," June 2001.
7. 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).

Table B 3.7.2-1

Heat Sink Group	Established Design Temperature
CRHA Heat Sink Group 1	
Control Room Habitability Area: Main control room panel Rooms: No 3270, 3272, 3271, 3201, 3202, 3273, 3206, 3205, 3204, 3275, 3207, 3208	23.3ºC (74ºF)
Corridors: [1] Rooms 3100, 3101 and Rooms 3200,3203, 3277, 3274	25.6ºC (78ºF)
HVAC chases: [1] Rooms 3251, 3260	25.6ºC (78ºF)
CRHA Heat Sink Group 2	
Q-DCIS equipment rooms: Rooms No 3110, 3120, 3130 and 3140	25.6ºC (78ºF)
N-DCIS equipment rooms: Rooms 3301, 3302, 3303, 3300	25.6ºC (78ºF)
Electrical chases: [1] Rooms 3250, 3261	25.6ºC (78ºF)
CRHA Heat Sink Group 3	
HVAC equipment rooms: Rooms 3401, 3402, 3403, 3404	40ºC (104ºF)
Safety Portions of CRHAVS: Rooms 3406, 3407	40 ºC (104ºF)

1. Access corridors, electrical chases, and HVAC chases, although part of the CRHA heat sink, are not monitored because these areas do not contain heat sources and their temperatures are assumed to match the average of the associated group.

B 3.7 PLANT SYSTEMS

B 3.7.3 Main Condenser Offgas

BASES

BACKGROUND	During unit operation, steam from the low-pressure turbine is exhausted directly into the condenser. Air and noncondensible gases are collected in the condenser, and then exhausted through the steam jet air ejectors (SJAEs) to the Main Condenser Offgas System. The offgas from the main condenser normally includes radioactive gases. The Main Condenser Offgas System has been incorporated into the unit design to reduce the gaseous radwaste emission. This system uses a catalytic recombiner to recombine radiolytically dissociated hydrogen and oxygen. The gaseous mixture is cooled by the offgas condenser, and the water and condensibles are stripped out by the offgas condenser and moisture separator. The radioactivity of the remaining gaseous mixture (i.e., the offgas recombiner effluent) is monitored downstream of the moisture separator prior to entering the holdup line.
APPLICABLE SAFETY ANALYSES	The main condenser offgas gross gamma activity rate is an initial condition of the Waste Gas System leak or failure event as discussed in Sections 11.3.7 and 15.0.3.4.7 (Refs. 1 and 2, respectively). The analysis assumes inadvertent operator action with the bypass of the delay charcoal beds leading to a direct release of radioactive noble gases from the Main Condenser Offgas System. The gross gamma activity rate is controlled to ensure that during the event, the calculated offsite doses using the annual average atmospheric dispersion factor will be well within the acceptance criterion of 25 mSv (2.5 rem) TEDE (Ref. 3). The main condenser offgas limits satisfy Criterion 2 of 10 CFR 50.36(c)(2)(ii).
LCO	To ensure compliance with the assumptions of the Waste Gas System leak or failure event (Refs. 1 and 2), the fission product release rate should be consistent with a noble gas release to the reactor coolant of 100 μCi/second/Mwt after decay of 30 minutes. The LCO is established consistent with this requirement (4500 MWt x 100 μCi/second/MWt = 450 mCi/second).

BASES

APPLICABILITY

The LCO is applicable when steam is being exhausted to the main condenser and the resulting noncondensibles are being processed via the Main Condenser Offgas System. This occurs during MODE 1, and during MODES 2, 3, and 4 with any main steam line not isolated and the SJAE in operation. In MODES 5 and 6, steam is not being exhausted to the main condenser and the requirements are not applicable.

ACTIONS

A.1

If the offgas radioactivity rate limit is exceeded, 72 hours is allowed to restore the gross gamma activity rate to within the limit. The 72-hour Completion Time is reasonable, based on engineering judgment considering the time required to complete the Required Action, the large margins associated with permissible dose and exposure limits, and the low probability of a Waste Gas System leak or failure event occurring.

B.1, B.2, B.3.1, and B.3.2

If the gross gamma activity rate is not restored to within the limits within the associated Completion Time, all main steam lines or the SJAE must be isolated. This isolates the Main Condenser Offgas System from the source of the radioactive steam. The main steam lines are considered isolated if at least one main steam isolation valve in each main steam line is closed, and at least one main steam line drain valve in each drain line is closed. The 12-hour Completion Time is reasonable, based on operating experience, to perform the actions from full power conditions in an orderly manner and without challenging unit systems.

An alternative to Required Action B.1 or B.2 is to place the unit 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 12 hours and in MODE 5 within 36 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required unit conditions from full power conditions in an orderly manner and without challenging unit systems.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.7.3.1

This SR, on a 31-day Frequency, requires an isotopic analysis of an offgas sample to ensure that the required limits are satisfied. The noble gases to be sampled are Xe-133, Xe-135, Xe-138, Kr-85, Kr-87, and Kr-88. If the measured rate of radioactivity increases significantly (by ≥ 50% after correcting for expected increases due to changes in THERMAL POWER), an isotopic analysis is also performed, within 4 hours after the increase is noted, to ensure that the increase is not indicative of a sustained increase in the radioactivity rate. The 31-day Frequency is adequate in view of other instrumentation that continuously monitors the offgas, and is acceptable based on operating experience.

This SR is modified by a Note indicating that the SR is not required to be performed until 31 days after any main steam line is not isolated and the SJAE is in operation. Only in this condition can radioactive fission gases be in the Main Condenser Offgas System at significant rates.

REFERENCES

1. Section 11.3.7.
2. Section 15.0.3.4.7.
3. NUREG-0800, Branch Technical Position 11-5, Revision 3, March 2007.

B 3.7 PLANT SYSTEMS

B 3.7.4 Main Turbine Bypass System

BASES

BACKGROUND

The Main Turbine Bypass System is designed to control steam pressure when reactor steam generation exceeds turbine requirements during unit startup, sudden load reduction, and cooldown. It allows excess steam flow from the reactor to the condenser without going through the turbine. The bypass capacity of the system is 110% of the Nuclear Steam Supply System rated steam flow. Sudden load reductions within the capacity of the steam bypass can be accommodated without reactor scram.

The Main Turbine Bypass System consists of turbine bypass valves (TBVs) connected to the main steam lines between the main steam isolation valves (MSIVs) and the turbine stop valves. The turbine hydraulic fluid power unit supplies high-pressure fluid to sequentially open the TBVs and can be isolated from supplying high-pressure fluid to the turbine valves while supplying hydraulic fluid to the TBVs. The TBVs are controlled by the pressure regulation function of the Steam Bypass and Pressure Control (SB&PC) System, as discussed in Reference 1. The TBVs are normally closed, and the pressure regulator controls the turbine control valves (TCVs), directing all steam flow to the turbine. The TBVs are opened by redundant signals from the SB&PC System, which uses a triply redundant digital control system, whenever the actual steam pressure exceeds the preset steam pressure by a small margin. This bypass demand opens the TBVs in sequence as necessary to control pressure. Additionally, the TBVs are equipped with fast acting solenoid valves to allow rapid opening of the valves for the generator load rejection with turbine bypass, generator load rejection with a single failure in the turbine bypass system, turbine trip with turbine bypass, and turbine trip with a single failure in the turbine bypass system events (Ref. 2). No credible single failure in the control system results in a minimum demand to all TCVs and TBVs, or in disabling more than 50% of the TBVs. When the TBVs open, the steam flows from the bypass valves to the condenser through connecting piping and pressure reducers.

BASES

APPLICABLE SAFETY ANALYSES	The Main Turbine Bypass System is assumed to function during transient events that could result in increase in reactor pressure (i.e., closure of one TCV, generator load rejection with turbine bypass, generator load rejection with a single failure in the turbine bypass system, turbine trip with turbine bypass, turbine trip with a single failure in the turbine bypass system, closure of one MSIV, and feedwater controller failure – maximum demand). Opening of the bypass valves during the pressurization event mitigates the increase in reactor vessel pressure, which affects the MCPR during the event. [An inoperable Main Turbine Bypass System may result in an MCPR penalty.]
COL 16.0-1-A 3.7.4-1	The Main Turbine Bypass System satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).
LCO	The Main Turbine Bypass System is required to be OPERABLE to limit peak pressure in the main steam lines and maintain reactor pressure within acceptable limits during events that cause rapid pressurization, such that the Fuel Cladding Integrity Safety Limit (FCISL) is not exceeded. [With the Main Turbine Bypass System inoperable, modifications to the MCPR limits (LCO 3.2.2, "MINIMUM CRITICAL POWER RATIO (MCPR)") may be applied to allow continued operation. The MCPR limit for the inoperable Main Turbine Bypass System is specified in the COLR.]
COL 16.0-1-A 3.7.4-1	An OPERABLE Main Turbine Bypass System requires the TBVs to open in response to increasing main steam line pressure or in the fast opening mode, as applicable. This response is within the assumptions of the applicable analyses (Ref. 3).
APPLICABILITY	The Main Turbine Bypass System is required to be OPERABLE at ≥ 25% RTP to ensure that the FCISL and the cladding 1% plastic strain limit are not violated during transient events such as the generator load rejection with turbine bypass event. As discussed in the Bases for LCO 3.2.2, sufficient margin to these limits exists below 25% RTP. Therefore, these requirements are only necessary when operating at or above this power level.

BASES

ACTIONS

A.1

COL 16.0-1-A
3.7.4-1

If the Main Turbine Bypass System is inoperable (one or more TBVs inoperable)[, or the MCPR limits for an inoperable Main Turbine Bypass System, as specified in the COLR, are not applied], the assumptions of the design basis transient analysis may not be met. Under such circumstances, prompt action should be taken to restore the Main Turbine Bypass System to OPERABLE status or adjust the MCPR limits accordingly. The 2-hour Completion Time is reasonable, based on the time to complete the Required Action, and the low probability of an event occurring during this period requiring the Main Turbine Bypass System.

B.1

If Required Action A.1 and associated Completion Time cannot be met, THERMAL POWER must be reduced to < 25% RTP. As discussed in the Applicability section, operation at < 25% RTP results in sufficient margin to the required limits, and the Main Turbine Bypass System is not required to protect fuel integrity during transient events such as the generator load rejection with turbine bypass event. The 4-hour Completion Time is reasonable, based on operating experience, to reach the required unit condition from full power conditions in an orderly manner and without challenging unit systems.

SURVEILLANCE REQUIREMENTS

SR 3.7.4.1

COL 16.0-1-A
3.7.4-2

Cycling each TBV through one complete cycle of full travel demonstrates that the valves are mechanically OPERABLE and will function when required. The [31 day Frequency is based on engineering judgment, is consistent with the procedural controls governing valve operation,] and ensures correct valve positions. Therefore, the Frequency is concluded to be acceptable from a reliability standpoint.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.7.4.2

The Main Turbine Bypass System is required to actuate automatically to perform its designed function. This SR demonstrates that with the required system initiation signals, the TBVs will actuate to their required position. The 24-month Frequency is based on the need to perform this Surveillance under the conditions that apply during a unit outage and because of the potential for an unplanned transient if the Surveillance were performed with the reactor at power. Operating experience has shown the 24-month Frequency, which is based on the refueling cycle, is acceptable from a reliability standpoint.

SR 3.7.4.3

This SR ensures that the TURBINE BYPASS SYSTEM RESPONSE TIME is in compliance with the assumptions of the appropriate safety analysis. The response time limits are specified in Reference 4. The 24-month Frequency is based on the need to perform this Surveillance under the conditions that apply during a unit outage and because of the potential for an unplanned transient if the Surveillance were performed with the reactor at power. Operating experience has shown the 24-month Frequency, which is based on the refueling cycle, is acceptable from a reliability standpoint.

REFERENCES

1. Section 7.7.5.

2. Section 10.4.4.

3. Section 15.2.2.

4. Chapter 15, Table 15.2-1

B 3.7 PLANT SYSTEMS

B 3.7.5 Fuel Pool Water Level and Temperature

BASES

BACKGROUND	The minimum water level in the deep pit area of the reactor building buffer pool and in the fuel building spent fuel storage pool bounds the assumptions of iodine decontamination factors following a fuel handling accident. The water in these pools also provides a large capacity heat sink in the event the Fuel and Auxiliary Pools Cooling System (FAPCS) is unavailable. The minimum water level and assumed initial pool temperature for a postulated loss of FAPCS are found in Reference 5. A general description of the reactor building buffer pool and fuel building spent fuel storage pool design is found in Section 9.1.2 (Ref. 1). The assumptions of the fuel handling accident are found in Section 15.4.1 (Ref. 2).
APPLICABLE SAFETY ANALYSES	The water level above the irradiated fuel assemblies is an explicit assumption of the fuel handling accident. A fuel handling accident is evaluated to ensure the radiological consequences (whole-body dose or its equivalent to any part of the body calculated at the exclusion area and low population zone boundaries) are < 0.063 Sv (6.3 rem) total effective dose equivalent (TEDE) and < 0.05 Sv (5.0 rem) TEDE in the control room as required by 10 CFR 52.47(a)(2)(iv) (Ref. 3) and Regulatory Guide 1.183 (Ref. 4) acceptance criteria. A fuel handling accident is assumed to damage all of the fuel rods in two (2) fuel assemblies as discussed in References 2 and 4. The fuel handling accident is evaluated for the dropping of an irradiated fuel assembly onto the reactor core which bounds the consequences of dropping an irradiated fuel assembly onto stored fuel bundles. The justification for the bounding analysis used, initial assumptions of the analysis, and consequences of a fuel handling accident inside the reactor building are documented in Reference 2. The water level above the irradiated fuel assemblies provides for absorption of water-soluble fission-product gases and transport delays of soluble and insoluble gases that must pass through the water before being released to the reactor building or fuel building atmosphere. This absorption and transport delay reduces the potential radioactivity of the release during a fuel handling accident.

BASES

APPLICABLE SAFETY ANALYSES (continued)

In addition to mitigating the effects of a fuel handling accident, the required minimum water level and maximum water temperature in the spent fuel storage pool and buffer pool provide a large capacity heat sink in the event FAPCS is unavailable. For both pools, the water levels and free volumes are sufficient to ensure that following a loss of active cooling without makeup that persists for 72 hours, the water levels in the pools remain above the top of the irradiated fuel assemblies. The minimum water level required for the buffer pool is less than that required for the spent fuel pool, however the bounding value of 10.26 m is utilized for this LCO.

The fuel pool water level and temperature satisfy Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

The water level limit preserves the assumption of the fuel handling accident analysis (Ref. 2) and loss of FAPCS (Ref. 5). The water temperature limit preserves the assumption of loss of FAPCS (Ref. 5).

APPLICABILITY

This LCO applies whenever irradiated fuel assemblies are being moved or stored in the associated fuel storage racks since the potential for a release of fission-products exists.

ACTIONS

A.1

When the initial conditions for an accident cannot be met, steps should be taken to preclude the accident from occurring. With either fuel pool level less than required, the movement of irradiated fuel assemblies in the associated storage pool is immediately suspended. Suspension of this activity shall not preclude completion of movement of an irradiated fuel assembly to a safe position. This effectively precludes a spent fuel handling accident from occurring.

This action is also appropriate when fuel pool average water temperature is not within limit since adding heat load to a pool with reduced capacity as a heat sink should not be performed.

BASES

ACTIONS (continued)

A.2

If the water level in the spent fuel storage pool or buffer pool is < 10.26 m (33.7 ft) above the top of the irradiated fuel assemblies, or if the average water temperature is > 60°C (140°F), the heat capacity of the pool may be less than that assumed in the event of a loss of FAPCS. In this case, action must be initiated within 1 hour to restore the water level and temperature to within limit. Action must continue until the parameter is restored to within the applicable limit.

The Completion Time of 1 hour ensures prompt action will be taken to compensate for a degraded condition.

Required Actions A.1 and A.2 have been modified by a Note indicating that LCO 3.0.3 does not apply. If moving irradiated fuel assemblies while in MODE 1, 2, 3, or 4, the fuel movement is independent of reactor operations. Fuel pool cooling requirements are also independent of reactor operations. Therefore, inability to suspend movement of irradiated fuel assemblies or to initiate restoration of fuel pool water level and temperature to within limit is not a sufficient reason to require a reactor shutdown.

SURVEILLANCE REQUIREMENTS

SR 3.7.5.1

This SR verifies sufficient water is available to mitigate the consequences of a fuel handling accident or a loss of cooling in the spent fuel storage pool or buffer pool. The water level in the spent fuel storage pool and buffer pool must be checked periodically. The 7-day Frequency is acceptable, based on operating experience, considering that the water volume in the pool is normally stable and water level changes are controlled by unit procedures.

During refueling operations, the level above the top of the RPV flange is verified every 24 hours in accordance with SR 3.9.6.1.

SR 3.7.5.2

This SR verifies that the average water temperature in the spent fuel storage pool and buffer pool is low enough to mitigate the consequences of a loss of cooling. The temperature in the spent fuel storage pool and buffer pool must be checked periodically. The 7-day Frequency is

BASES

SURVEILLANCE REQUIREMENTS (continued)

acceptable considering the alarms and indications available to alert the operator to abnormal conditions associated with the fuel pool and FAPCS.

REFERENCES

1. Section 9.1.2.
2. Section 15.4.1.
3. 10 CFR 52.47(a)(2)(iv).
4. Regulatory Guide 1.183, July 2000.
5. Section 9.1.3.2.

B 3.7 PLANT SYSTEMS

B 3.7.6 Selected Control Rod Run-In (SCRRI) and Select Rod Insert (SRI) Functions

BASES

BACKGROUND

Selected Control Rod Run-In (SCRRI) function logic is performed when the Rod Control and Information System (RC&IS) performs 2/3 voting on a Selected Control Rod Run-in/Select Rod Insert (SCRRI/SRI) signal from the Diverse Protection System (DPS) (Ref. 1). RC&IS provides for electrical insertion of selected control rods: 1) for mitigation of a loss of feedwater heating event; or 2) for providing needed power reduction after occurrence of a load rejection event or a turbine trip event. The Automated Thermal Limit Monitor (ATLM) provides an additional SCRRI/SRI signal to RC&IS for mitigation of a loss of feedwater heating event.

RC&IS utilizes a dual-redundant architecture of two independent channels for normal monitoring of control rod positions and executing normal control rod movement commands. Under normal conditions, each channel receives separate input signals and both channels perform the same functions. For the Fine Motion Control Rod Drive (FMCRD) emergency insertion functions (scram-follow, FMCRD run-in, and SCRRI), 3-out-of-3 logic is used in the induction motor controller logic with the additional input signal coming from the associated emergency rod insertion panels. An automatic single channel bypass feature (only activated when an emergency insertion function is activated) is also provided to assure high availability for the emergency insertion functions when a single channel failure condition exists.

Failure or malfunction of RC&IS has no impact on the hydraulic scram function of the CRDs. The circuitry for normal insertion and withdrawal of control rods in RC&IS is completely independent of the Reactor Protection System (RPS) circuitry controlling the scram valves. This separation of the RPS scram and RC&IS normal rod control functions prevents failure in the RC&IS circuitry from affecting the scram circuitry.

Select Rod Insert (SRI) function logic in DPS produces the automatic SRI command signal to the scram timing test panel (Ref. 1). Similarly, 2/3 voting is performed by the DPS on the hard-wired turbine trip and load reject signals from the turbine control system to produce an automatic SRI command signal to the scram timing test panel. The scram timing test panel provides for hydraulic scram insertion of selected control rods: 1) for mitigation of a loss of feedwater heating event; or 2) for providing

BASES

BACKGROUND (continued)

needed power reduction after occurrence of a load rejection event or a turbine trip event. ATLM provides an additional SCRRI/SRI signal to RC&IS for mitigation of a loss of feedwater heating event.

DPS utilizes a triplicate redundant system to produce the SRI signal to the scram timing test panel, which on a valid SRI initiation signal causes all the hydraulic control unit (HCU) solenoid return line switches for the control rods selected for SRI to open, resulting in a hydraulic scram of those control rods. The scram timing test panel allows specific HCUs associated with the predetermined SRI control rods to be selected on the scram timing test panel video display unit interface.

Failure or malfunction of DPS or the scram timing test panel has no impact on the hydraulic scram function of the CRDs. The circuitry for emergency electrical insertion and SRI hydraulic insertion of control rods in DPS and the scram timing test panel is completely independent of the RPS circuitry controlling the scram valves. This separation of the RPS scram and the DPS and scram timing test panel control rod functions prevents failure in the DPS and scram timing test panel circuitry from affecting the scram circuitry.

APPLICABLE SAFETY ANALYSES

The SCRRI and SRI functions are assumed to function during transient events that could result in a decrease in core coolant temperature or increase in reactor pressure (i.e., loss of feedwater heating, generator load rejection, and turbine trip). Power reduction from the electrical run-in and hydraulic insertion of selected control rods during these events mitigates the decrease in the MCPR during the event.

COL 16.0-1-A 3.7.6-1

[An inoperable SCRRI or SRI function may result in an MCPR penalty.]

The SCRRI and SRI functions satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO

The SCRRI and SRI functions are required to be OPERABLE to limit decrease in MCPR within acceptable limits during events that cause rapid increase in core reactivity, such that the Fuel Cladding Integrity Safety Limit (FCISL) is not exceeded. [With the SCRRI or SRI functions inoperable, modifications to the MCPR limits (LCO 3.2.2, "MINIMUM CRITICAL POWER RATIO (MCPR)") may be applied to allow continued operation. The MCPR limit for the inoperable SCRRI function and/or SRI function is specified in the COLR.]

COL 16.0-1-A 3.7.6-1

OPERABLE SCRRI and SRI functions actuate in response to a loss of feedwater heating, or a turbine trip or load reject, as applicable. This response is within the assumptions of the applicable analyses (Ref. 2). The specific control rods and insertion limits applicable to the SCRRI and SRI functions are specified in the COLR.

APPLICABILITY

The SCRRI and SRI functions are required to be OPERABLE at ≥ 25% RTP to ensure that the FCISL and the cladding 1% plastic strain limit are not violated during transient events such as the loss of feedwater heating event. As discussed in the Bases for LCO 3.2.2, sufficient margin to these limits exists below 25% RTP. Therefore, these requirements are only necessary when operating at or above this power level.

ACTIONS

A.1

If the SCRRI or SRI function is inoperable (including one or more selected control rods inoperable)[, or the MCPR limits for an inoperable SCRRI and/or SRI function, as specified in the COLR, are not applied], the assumptions of the design basis transient analysis may not be met. Under such circumstances, prompt action should be taken to restore the SCRRI and SRI functions to OPERABLE status [or adjust the MCPR limits accordingly]. The 2-hour Completion Time is reasonable, based on the time to complete the Required Action, and the low probability of an event occurring during this period requiring the SCRRI and SRI functions.

COL 16.0-1-A 3.7.6-1

BASES

ACTIONS (continued)

B.1

If Required Action A.1 and associated Completion Time cannot be met, THERMAL POWER must be reduced to < 25% RTP. As discussed in the Applicability section, operation at < 25% RTP results in sufficient margin to the required limits, and the SCRRI and SRI functions are not required to protect fuel integrity during transient events such as the loss of feedwater heating event. The 4-hour Completion Time is reasonable, based on operating experience, to reach the required unit condition from full power conditions in an orderly manner and without challenging unit systems.

SURVEILLANCE REQUIREMENTS

SR 3.7.6.1

The control rods assumed to insert, and the final control rod pattern achieved, to accomplish the SCRRI and SRI functions are analyzed for each fuel cycle and are documented in the COLR in accordance with Specification 5.6.3. The Surveillance Requirements of LCO 3.1.3, "Control Rod OPERABILITY," made applicable to the required SCRRI and SRI function control rods are required to establish this LCO is being met.

SR 3.7.6.2

Fine Motion Control Rod Drive (FMCRD) electrical insertion capability for the SCRRI function is verified by ensuring that power is available to the selected FMCRDs. The 7-day Frequency is adequate since breaker position is not likely to change without the operator being aware of it and because the FMCRD electrical power availability status is displayed in the control room.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.7.6.3

The SCRRI function is required to automatically electrically insert selected control rods to perform its designed function. This SR demonstrates that with the required system initiation signals, the SCRRI function will electrically insert the selected control rods to their required position. The 24-month Frequency is based on the need to perform this Surveillance under the conditions that apply during a unit outage and because of the potential for an unplanned transient if the Surveillance were performed with the reactor at power. Operating experience has shown the 24-month Frequency, which is based on the refueling cycle, is acceptable from a reliability standpoint.

SR 3.7.6.4

The SRI function is required to automatically hydraulically insert selected control rods to perform its designed function. This SR demonstrates that with the required system initiation signals, the SRI function will hydraulically insert the selected control rods to their required position. The 24-month Frequency is based on the need to perform this Surveillance under the conditions that apply during a unit outage and because of the potential for an unplanned transient if the Surveillance were performed with the reactor at power. Operating experience has shown the 24-month Frequency, which is based on the refueling cycle, is acceptable from a reliability standpoint.

SR 3.7.6.5

This SR ensures that the FMCRD electrical insertion rate over the required insertion range for each SCRRI control rod required in accordance with the COLR is in compliance with the assumptions of the appropriate safety analysis. The 24-month Frequency is based on the need to perform this Surveillance under the conditions that apply during a unit outage and because of the potential for an unplanned transient if the Surveillance were performed with the reactor at power. Operating experience has shown the 24-month Frequency, which is based on the refueling cycle, is acceptable from a reliability standpoint.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.7.6.6

CHANNEL CALIBRATION is a complete check of the instrument loop and the sensor. This test verifies that the channel responds to the measured parameters within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to the required nominal trip setpoint within the "as-left tolerance" to account for instrument drifts between successive calibrations consistent with the methods and assumptions required by the Setpoint Control Program. The Frequency is based upon the assumption of a 24-month calibration interval in the determination of the magnitude of equipment drift in the setpoint analysis.

REFERENCES

1. Sections 7.1 and 7.7.
2. Section 15.2.

B 3.8 ELECTRICAL POWER SYSTEMS

B 3.8.1 DC Sources - Operating

BASES

BACKGROUND

The DC Sources supply the emergency 250 VDC power to the DC to AC inverters, which are used to provide Uninterruptible 120 VAC Power during all modes of operation. Uninterruptible 120 VAC Power supplies all safety-related loads, including the Safety-Related Distributed Control and Information System (Q-DCIS) and the control power for safety-related systems. The DC sources are designed to have sufficient capacity, independence, redundancy, and testability to perform their safety functions when any three of the four divisions are available, assuming a single failure of one of the three required divisions. The DC electrical power system conforms to the recommendations of Regulatory Guide 1.6 (Ref. 1) and IEEE-308 (Ref. 2).

There are two DC Sources for each of the four divisions of the DC Electrical Power Distribution system. Each of the two DC Sources in each division includes a 250 V battery, an associated battery charger (the normal charger), and all the associated control equipment and interconnecting cabling. The battery and battery charger for each DC source are connected to an associated 250 VDC bus. Each division also includes a third battery charger (the standby charger). The standby battery charger may be connected to either of the DC Sources in that division to replace the normal battery charger. The standby battery charger can also be used to charge the battery in either DC source, even if the battery is disconnected from its associated 250 VDC bus.

Each division has two 120 VAC Uninterruptible AC Power inverters, which receive power from an associated rectifier or battery and battery charger. Each rectifier receives 480 VAC normal power from the isolation power center of that division and converts it to 250 VDC. The 480 VAC/250 VDC rectifier and a safety-related 72-hour battery and battery charger of that division supply 250 VDC emergency power through diodes to a common inverter. The output diodes for battery chargers and safety-related rectifiers isolate the output of each required battery from an associated 480 VAC isolation power center bus that is de-energized or has degraded voltage.

BASES

BACKGROUND (continued)

The plant design and circuit layout of the DC systems provide physical separation of the equipment, cabling, and instrumentation essential to plant safety to ensure that a single failure in one division does not cause a failure in a redundant division. There is no sharing between redundant divisions such as batteries, battery chargers, or distribution panels. The 250 V batteries for each division are separately housed in a ventilated room apart from their chargers, distribution buses, and ground detection panels. Equipment for each Division of DC distribution is located in an area separated physically from the other divisions. All the components of 250 VDC sources are housed in Seismic Category I structures.

COL 16.0-1-A 3.8.1-5

The batteries are sized so that the batteries in any two of the four divisions have sufficient stored capacity, without recharging, to achieve and maintain safe shutdown conditions for 72 hours following any design basis event. The minimum battery terminal voltage at the end of the discharge period is 210 volts (1.75 volts per cell [Vpc]). The batteries are sized so that the sum of the required loads does not exceed [80%] of the battery ampere-hour rating, or warranted capacity at end-of-installed-life with 100% design demand. Batteries are sized for the DC load in accordance with IEEE Standard 485 (Ref. 3) and include margin to compensate for uncertainty in determining the battery state of charge. The battery banks are designed to permit the replacement of individual cells.

Either the normal or the standby battery charger associated with each battery is capable of recharging its battery from the design minimum charge to fully charged condition within 24 hours while supplying the full load of the associated DC source (Ref. 4).

The battery charger is normally in the float-charge mode supplying the connected loads (when those loads are not being supplied via the 480 VAC rectifier) 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.

The charger can be placed at a higher voltage than the float mode for battery equalize and following a battery discharge for more rapid recharge. 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

BASES

BACKGROUND (continued)

approaches the charger voltage setpoint. Charging current then reduces exponentially during the remainder of the recharge cycle. The 72-hour batteries have recharge efficiencies such that once approximately 105% to 110% 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.

APPLICABLE SAFETY ANALYSES

The initial conditions of Design Basis Accident (DBA) and transient analyses in Chapter 6 (Ref. 5) and Chapter 15 (Ref. 6) assume that Engineered Safety Feature (ESF) systems are OPERABLE. The DC Sources provide emergency 250 VDC power to the DC Electrical Power Distribution System, which supplies power through the inverters to the Uninterruptible 120 VAC Power buses. Uninterruptible 120 VAC Power supports Q-DCIS and the control power for safety-related systems.

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 OPERABILITY of the DC Sources needed to support the three divisions of DC and Uninterruptible AC Electrical Power Distribution required by LCO 3.8.6, "Distribution Systems – Operating," so that at least two divisions remain OPERABLE during accident conditions in the event of:

a. An assumed loss of all offsite and onsite AC power sources; and

b. A worst-case single failure.

The DC Sources satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

DC Sources are required to be OPERABLE to support the three Divisions of DC and Uninterruptible AC Electrical Power Distribution required by LCO 3.8.6, "Distribution Systems – Operating." Each required division is required to have two DC Sources, with each DC source consisting of the 250 V battery, the associated battery charger (either the normal or the standby charger), and all the associated control equipment and interconnecting cabling.

BASES

LCO (continued)

Three of the four Divisions of DC Sources 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 Design Basis Accident (DBA). Loss of one of the required Divisions of DC Sources does not prevent the minimum safety function from being performed (Ref. 4).

APPLICABILITY

The DC 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; and

b. Adequate core cooling is provided, and containment integrity and other vital functions are maintained in the event of a postulated DBA.

The DC electrical power requirements for MODES 5 and 6 are addressed in the Bases for LCO 3.8.2, "DC Sources - Shutdown."

ACTIONS

A.1

Condition A represents one DC Source inoperable on one required division (i.e., one required battery charger, one battery, or one battery and its associated required battery charger inoperable). In this Condition, the remaining OPERABLE battery and battery charger in the associated division can continue to support the immediate safety-related function following a transient event or DBA concurrent with a loss of offsite and onsite AC power, however, it may not have adequate capacity to support the associated division of the DC Electrical Power Distribution system for the required duration of 72 hours.

With one DC Source inoperable on one required division, the remaining required divisions of DC and Uninterruptible AC Electrical Power have the capacity to support a safe shutdown and to mitigate an accident condition even with an additional single failure, albeit for less than the design basis

BASES

ACTIONS (continued)

72 hours. In this condition, continued power operation should not exceed 72 hours. The 72 hour Completion Time for the restoration of the inoperable DC source is consistent with the time allowed for one inoperable DC Electrical Power Distribution bus.

B.1

Condition B represents both DC Sources inoperable on one required division. In this Condition, the affected division of the DC Sources may not have adequate capacity to support the associated division of the DC Electrical Power Distribution system following a transient event or DBA concurrent with a loss of offsite and onsite AC power.

With both DC Sources inoperable on one required division, the two remaining required divisions of DC and Uninterruptible AC Electrical Power have the capacity to support a safe shutdown and to mitigate an accident condition even if power is lost to the supporting isolation power center buses. However, a single failure could result in the loss of minimum necessary 250 VDC subsystems. Therefore, continued power operation should not exceed 8 hours. The 8 hour Completion Time for the restoration of an inoperable DC source is consistent with the time allowed for an inoperable division of DC Electrical Power Distribution.

C.1 and C.2

When one or more DC Sources on two or more required divisions are inoperable, the remaining DC Sources may not have the capacity to supply power to the divisions of the DC Electrical Power Distribution system for the required duration of 72 hours following a transient event or DBA, concurrent with a loss of offsite and onsite AC power. If the Required Actions for restoration cannot be met within the specified Completion Times, the plant remains vulnerable to a single failure that could impair the capability to reach safe shutdown or to mitigate an accident condition. Therefore, the unit 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 12 hours and to MODE 5 within

BASES

ACTIONS (continued)

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 3.8.1.1

COL 16.0-1-A 3.8.1-4

Verifying battery terminal voltage while on float charge helps to ensure the effectiveness of the battery chargers, which support the ability of the batteries to perform their intended function. Float charge is the condition in which the charger is supplying the continuous charge required to overcome the internal losses of a battery and maintain the battery in a 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 ([2.22 Vpc or 266.4 V at 25°C (77°F) at the battery terminals]). This voltage maintains the battery in a condition that supports maintaining battery life. The 7 day Frequency is consistent with manufacturer recommendations.

SR 3.8.1.2

This SR verifies the design capacity of the battery chargers. According to Regulatory Guide 1.32 (Ref. 7), 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.

COL 16.0-1-A 3.8.1-1

This SR provides two options. One option requires that each battery charger be capable of supplying 500 amps at the minimum established float voltage [for 4 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].

BASES

SURVEILLANCE REQUIREMENTS (continued)

The other option requires that each battery charger be capable of recharging the battery after a service test coincident with supplying the largest combined demands of the various continuous steady state loads (irrespective of the status of the plant during which these demands occur). This level of loading may not normally be available following the battery service test and will need to be supplemented with additional loads. The duration for this test may be longer than the charger sizing criteria since the battery recharge is affected by float voltage, temperature, and the exponential decay in charging current. The battery is recharged when the requirements of SR 3.8.3.1 are met.

The Surveillance Frequency is acceptable, given the unit conditions required to perform the test and the other administrative controls existing to ensure adequate charger performance during these 24-month intervals. In addition, this Frequency is intended to be consistent with expected fuel cycle lengths.

<u>SR 3.8.1.3</u>

A battery-service test is a special test of the battery's capability, as found, to satisfy the design requirements (battery duty cycle) of the 250 VDC power system. The discharge rate and test length corresponds to the design duty cycle requirements. The Surveillance Frequency of 24 months is consistent with the recommendations of Regulatory Guide 1.32 (Ref. 7).

<u>SR 3.8.1.4</u>

Operability of a DC Source requires that the output diodes for the associated battery chargers and safety-related rectifiers prevent reverse current flow from the DC Source to the associated isolation power center bus when the isolation power center bus is de-energized or has degraded voltage. This function is required to prevent degraded conditions on the nonsafety-related AC power system from affecting the safety-related DC power system. This SR is not required for battery chargers and safety-related rectifiers that are not connected to the isolation power center bus. This SR is also not required for standby battery chargers that are not connected to the 250 VDC bus. The 24 month Frequency is based on engineering judgment.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.8.1.5

This SR verifies that each required DC Source can supply the 120 VAC Uninterruptible AC Power inverter for ≥ 4 hours. The 120 VAC Uninterruptible AC Power inverters are normally supplied by the safety-related rectifiers. The circuit between the DC source and the inverter is not tested during either the battery charger capacity test (SR 3.8.1.2) or the battery service test (SR 3.8.1.3). Failure of the circuit between the DC Source and the 120 VAC Uninterruptible AC Power inverter, which includes the diode that separates the output of the safety-related rectifier from the DC source, could prevent the DC source from performing its required safety function. The 24 month Frequency is based on engineering judgment.

REFERENCES

1. Regulatory Guide 1.6.
2. IEEE Standard 308.
3. IEEE Standard 485.
4. Chapter 8.
5. Chapter 6.
6. Chapter 15.
7. Regulatory Guide 1.32.

B 3.8 ELECTRICAL POWER SYSTEMS

B 3.8.2 DC Sources - Shutdown

BASES

BACKGROUND	A description of the DC Sources is provided in the Bases for LCO 3.8.1, "DC Sources - Operating."

APPLICABLE SAFETY ANALYSES

The initial conditions of Design Basis Accident (DBA) and transient analyses in Chapter 6 (Ref. 1) and Chapter 15 (Ref. 2) assume that Engineered Safety Feature (ESF) systems are OPERABLE. The DC Sources provide emergency 250 VDC power to the DC Electrical Power Distribution System, which supplies power through the inverters to the Uninterruptible 120 VAC Power buses. Uninterruptible 120 VAC Power supports Q-DCIS and the control power for safety-related systems.

The OPERABILITY of the DC sources is consistent with the initial assumptions of the accident analyses and the requirements for the supported systems' OPERABILITY. The OPERABILITY of the minimum DC sources during MODES 5 and 6 ensures that:

a. The facility can be maintained in the shutdown or refueling condition for extended periods,

b. Sufficient instrumentation and control capability is available for monitoring and maintaining the unit status, and

c. Adequate DC electrical power is provided to mitigate events postulated during shutdown, such as an inadvertent draindown of the vessel.

In general, when the unit is shutdown, the Technical Specifications requirements ensure that the unit has the capability to mitigate the consequences of postulated accidents. However, assuming a single failure and concurrent loss of all offsite or all onsite power is not required. The rationale for this is based on the fact that many Design Basis Accidents (DBAs) that are analyzed in MODES 1, 2, 3, and 4 have no specific analyses in MODES 5 and 6. Worst case bounding events are deemed not credible in MODES 5 and 6 because the energy contained within the reactor pressure boundary, reactor coolant temperature and pressure, and the corresponding stresses result in the probabilities of occurrence being significantly reduced or eliminated, and in minimal

BASES

APPLICABLE SAFETY ANALYSES (continued)

consequences. These deviations from DBA analysis assumptions and design requirements during shutdown conditions are allowed by the LCO for required systems.

The shutdown Technical Specification requirements are designed to ensure that the unit has the capability to mitigate the consequences of certain postulated accidents. Worst case DBAs that are analyzed for operating MODES are generally viewed not to be a significant concern during shutdown MODES due to the lower energies involved. The Technical Specifications therefore require a lesser complement of electrical equipment to be available during shutdown than is required during operating MODES. More recent work completed on the potential risks associated with shutdown, however, has found significant risk associated with certain shutdown evolutions. As a result, in addition to the requirements established in the Technical Specifications, the industry has adopted NUMARC 91-06, "Guidelines for Industry Actions to Assess Shutdown Management," as an industry initiative to manage shutdown tasks and associated electrical support to maintain risk at an acceptable low level. This may require the availability of additional equipment beyond that required by the shutdown Technical Specifications.

The DC Sources satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

DC Sources are required to be OPERABLE to support the DC and Uninterruptible AC Electrical Power Distribution Divisions required OPERABLE by LCO 3.8.7, "Distribution Systems - Shutdown." Each required DC source consists of the battery, the associated battery charger (either the normal or the standby charger), and all the associated control equipment and interconnecting cabling.

This LCO ensures the availability of sufficient 250 VDC power sources to operate the unit in a safe manner and to mitigate the consequences of postulated events during shutdown (e.g., inadvertent reactor vessel draindown).

BASES

APPLICABILITY

The DC Sources required to be OPERABLE in MODES 5 and 6 provide assurance that:

a. Required features to provide adequate coolant inventory makeup are available for the irradiated fuel assemblies in the core in case of an inadvertent draindown of the reactor vessel,

b. Required features necessary to mitigate the effects of events that can lead to core damage during shutdown are available, and

c. Instrumentation and control capability is available for monitoring and maintaining the unit in a cold shutdown condition or refueling condition.

The DC source requirements for MODES 1, 2, 3, and 4 are addressed in the Bases for LCO 3.8.1, "DC Sources- Operating."

ACTIONS

A.1

Condition A represents one DC Source inoperable on one required division (i.e., one required battery charger, one battery, or one battery and its associated required battery charger inoperable). In this Condition, the remaining OPERABLE battery and battery charger in the associated division can continue to support the immediate safety-related function following a transient event or DBA concurrent with a loss of offsite and onsite AC power, however, it may not have adequate capacity to support the associated division of the DC Electrical Power Distribution system for the required duration of 72 hours.

With one DC Source inoperable on one required division, the remaining required divisions of DC and Uninterruptible AC Electrical Power have the capacity to support a safe shutdown and to mitigate an accident condition even with an additional single failure, albeit for less than the design basis 72 hours. The 72 hour Completion Time for the restoration of the inoperable DC source is consistent with the time allowed for one inoperable DC Electrical Power Distribution bus.

BASES

ACTIONS (continued)

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

When two or more DC Sources being used to support the DC and Uninterruptible AC Electrical Power Distribution Divisions required by LCO 3.8.7 are inoperable, or if the Required Action and associated Completion Time of Condition A are not met, the remaining OPERABLE DC Sources may be capable of supporting sufficient systems to allow continuation of CORE ALTERATIONS and operations with a potential for draining the reactor vessel. By allowing the option to declare systems inoperable when the associated DC sources are inoperable, appropriate restrictions will be implemented in accordance with the ACTIONS of the affected system(s) LCO. In many instances, this would likely involve undesired administrative efforts. Therefore, the allowance for sufficiently conservative actions is made (i.e., to suspend CORE ALTERATIONS and any activities that could potentially result in inadvertent draining of the reactor vessel).

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 DC sources and to continue this action until restoration is accomplished in order to provide the necessary 250 VDC power to the plant safety systems.

The Completion Time of immediately is consistent with the required times for actions requiring prompt attention. The restoration of the required DC sources should be completed as quickly as possible in order to minimize the time during which the plant safety systems may be without sufficient power.

SURVEILLANCE REQUIREMENTS

SR 3.8.2.1

SR 3.8.2.1 requires performance of all Surveillances required by SR 3.8.1.1 through SR 3.8.1.5. Therefore, see the corresponding Bases for Specification 3.8.1 for a discussion of each SR.

BASES

REFERENCES

1. Chapter 6.
2. Chapter 15.

B 3.8 ELECTRICAL POWER SYSTEMS

B 3.8.3 Battery Parameters

BASES

BACKGROUND

This LCO delineates the limits on battery float current and float voltage, individual cell voltage, battery electrolyte temperature, and battery capacity for the DC source batteries. A discussion of these batteries and their OPERABILITY requirements is provided in the Bases for LCO 3.8.1, "DC Sources - Operating" and LCO 3.8.2, "DC Sources - Shutdown." In addition to the limitations of this Specification, the Battery Monitoring and Maintenance Program also implements a program specified in Specification 5.5.10 for monitoring various battery parameters.

COL 16.0-1-A 3.8.3-3

The battery cells are of flooded lead acid construction with a nominal specific gravity of [1.240]. This specific gravity corresponds to battery cells that have an open circuit battery voltage of approximately [249.6 V for 120 cell battery (i.e., cell voltage of 2.07 to 2.09 volts per cell (Vpc))]. The open circuit voltage is the voltage maintained when there is no charging or discharging. Once fully charged with its open circuit voltage [≥ 2.07 to 2.09 Vpc], the battery cell will maintain its capacity [for 30 days] without further charging per manufacturer's instructions. However, optimal long-term performance is obtained by maintaining a float voltage [2.22 to 2.24 Vpc at 25°C (77°F)]. This provides adequate over-potential, which [limits the formation of lead sulfate and self-discharge]. The nominal float voltage [of 2.23 Vpc at 25°C (77°F) corresponds to a total float voltage output of 267.6 V for a 120 cell battery as discussed in Chapter 8 (Ref. 1)].

APPLICABLE SAFETY ANALYSES

The initial conditions of Design Basis Accident (DBA) and transient analyses in Chapter 6 (Ref. 2) and Chapter 15 (Ref. 3) assume that Engineered Safety Feature (ESF) systems are OPERABLE. The DC Sources provide the emergency 250 VDC power to the DC Electrical Power Distribution System, which supplies power through the inverters to the Uninterruptible 120 VAC Power buses. Uninterruptible 120 VAC Power supports Q-DCIS and the control power for safety-related systems.

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 as described in the Bases for LCO 3.8.1, "DC Sources - Operating" and LCO 3.8.2, "DC Sources - Shutdown."

BASES

APPLICABLE SAFETY ANALYSES (continued)

Since battery parameters support the operation of the DC sources, they satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

Battery parameters must remain within acceptable limits to ensure availability of the required DC sources to shut down the reactor and maintain it in a safe condition after an anticipated operational occurrence or a postulated DBA. Battery parameter limits are conservatively established, allowing continued DC source function even with limits not met. Additional preventative maintenance, testing, and monitoring are performed in accordance with Specification 5.5.10, Battery Monitoring and Maintenance Program.

APPLICABILITY

The battery parameters are required solely for the support of the associated DC sources. Therefore, battery parameter limits are only required when the DC sources are required to be OPERABLE. Refer to Applicability discussion in Bases for LCO 3.8.1 and LCO 3.8.2.

ACTIONS

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

COL 16.0-1-A 3.8.3-3

With one or more cells in one or more batteries in one required division < [2.09] 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 3.8.1.1) and of the overall battery state of charge by monitoring the battery float charge current (SR 3.8.3.1). This assures that there is still sufficient battery capacity to perform the intended function. Therefore, the affected battery is not required to be considered inoperable solely as a result of one or more cells in one or more batteries < [2.09] V, and continued operation is permitted for a limited period up to 24 hours.

Since the Required Actions only specify "perform," a failure of SR 3.8.1.1 or SR 3.8.3.1 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 3.8.3.1 is failed, then there is not assurance that there is still sufficient battery capacity to perform the intended function and the battery must be declared inoperable immediately.

BASES

ACTIONS (continued)

B.1, B.2, C.1, and C.2

COL 16.0-1-A 3.8.3-1

One or two batteries on one required division with [float current > 30 amps] indicates that a partial discharge of the battery has occurred. This may be due to a temporary loss of a battery charger or possibly due to one or more battery cells in a low voltage condition reflecting some loss of capacity. Within 2 hours, verification of the required battery charger OPERABILITY is made by monitoring the battery terminal voltage. If the terminal voltage is found to be less than the minimum established float voltage there are two possibilities, the battery charger is inoperable or is operating in the current limit mode. 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 the allowed Completion Time (Required Actions B.2 and C.2). The battery must therefore be declared inoperable. LCO 3.8.1 addresses battery and charger inoperability.

COL 16.0-1-A 3.8.3-3

If the float voltage is found not to be satisfactory and there are one or more battery cells with float voltage less than [2.09] V, the associated "OR" statement in Condition G is applicable and the battery must be declared inoperable immediately. If float voltage is satisfactory and there are no cells less than [2.09] V, there is good assurance that, within 24 hours, the battery will be restored to its fully charged condition from any discharge that might have occurred due to a temporary loss of the battery charger. As described in Reference 1, either the normal or the standby battery charger associated with each battery is capable of recharging its battery from the design minimum charge to fully charged condition within 24 hours while supplying the full load of the associated DC source.

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 the allowed Completion Time.

BASES

ACTIONS (continued)

COL 16.0-1-A 3.8.3-1

If Condition B is entered due to one battery on one required division with [float current > 30 amps], then 24 hours is allowed for recharging the battery (Required Action B.2). As discussed previously, 24 hours should be adequate to restore the battery to its fully charged condition from any discharge that might have occurred due to a temporary loss of the battery charger. However, if Condition C is entered due to two batteries on one required division with [float current > 30 amps], then only 8 hours is allowed to recharge at least one of the batteries (Required Action C.2). 8 hours should be adequate to recharge a battery following a short duration discharge. The more conservative Completion Time of 8 hours is based on engineering judgment considering the increased risk that the affected division of the DC and Uninterruptible AC Electrical Power Distribution System may not have adequate capacity to support the immediate safety-related function following a transient event or DBA concurrent with a loss of offsite and onsite AC power.

COL 16.0-1-A 3.8.3-3

If the condition is due to one or more cells in a low voltage condition but still greater than [2.09] V and float voltage is found to be satisfactory, this is not indication of a substantially discharged battery and 24 hours (Required Action B.2 for one affected battery) or 8 hours (Required Action C.2 for two affected batteries) is a reasonable time prior to declaring the battery inoperable.

Since Required Actions B.1 and C.1 only specify "perform," a failure of SR 3.8.1.1 acceptance criteria does not result in the Required Action not met. However, if SR 3.8.1.1 is failed, the appropriate Condition(s), depending on the cause of the failure, is entered.

D.1, D.2, and D.3

With one or two batteries on one required division with one or more cells with electrolyte level above the top of the plates, but below the minimum established design limits, the batteries still retain sufficient capacity to perform the intended function. Therefore, the affected batteries are 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 D.1 and D.2 address this potential (as well as provisions in Specification 5.5.10, 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.

BASES

ACTIONS (continued)

Within 8 hours, level is required to be restored to above the top of the plates. The Required Action D.2 requirement to verify that there is no leakage by visual inspection and the Specification 5.5.10.b item to initiate action to equalize and test in accordance with manufacturer's recommendation are taken from Annex D of IEEE Standard 450 (Ref. 4). 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 battery may have to be declared inoperable and the affected cell(s) replaced.

E.1

With one or two batteries on one required division with battery pilot cell electrolyte temperature less than the minimum established design limit, 12 hours is allowed to restore the temperature to within limits. A low temperature results in reduced battery capacity. Since the battery is sized with margin, sufficient capacity exists to perform the intended function and the temporary degradation in battery capacity does not require the battery to be considered inoperable solely as a result of pilot cell electrolyte temperature not met.

F.1

With one or more required batteries in redundant required divisions 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 divisions are involved. With redundant divisions involved, this potential could result in a total loss of function on multiple systems that rely upon the batteries. The longer Completion Times specified for battery parameters on one required division not within limits are therefore not appropriate, and the parameters must be restored to within limits on all but one required division within 2 hours.

G.1

When any battery parameter is outside the allowances of the Required Actions for Condition A, B, C, D, E, or F, sufficient capacity to supply the maximum expected load requirement is not assured and the corresponding battery must be declared inoperable. Additionally, discovering one battery with one or more battery cells with float voltage less than [2.09] V and [float current > 30 amps] indicates that the battery

COL 16.0-1-A 3.8.3-3

COL 16.0-1-A 3.8.3-1

BASES

ACTIONS (continued)

capacity may not be sufficient to perform the intended functions. The battery must therefore be declared inoperable immediately.

SURVEILLANCE REQUIREMENTS

SR 3.8.3.1

COL 16.0-1-A 3.8.3-1

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. The [30 amp value] is based on returning the battery to [95]% charge and assumes a [5]% design margin for the battery. Use of float current to determine the state of charge of the battery is consistent with IEEE-450 (Ref. 4). The 7-day Frequency is consistent with IEEE-450 (Ref. 4).

COL 16.0-1-A 3.8.3-1

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 3.8.1.1. When this float voltage is not maintained, the Required Actions of LCO 3.8.1 are being taken. Furthermore, the float current limit [of 30 amps] is established based on the nominal float voltage value and is not directly applicable when this voltage is not maintained.

SR 3.8.3.2 and SR 3.8.3.5

COL 16.0-1-A 3.8.3-3

Optimal long-term battery performance is obtained by maintaining a float voltage within established design limits provided by the battery manufacturer, which corresponds to nominally [267.6 V at the battery terminals, or 2.23 Vpc at 25°C (77°F)]. This provides adequate over-potential, which [limits the formation of lead sulfate and self-discharge, which could eventually render the battery inoperable]. Float voltages below [2.13 Vpc at 25°C (77°F) but greater than 2.09 Vpc], are addressed in Specification 5.5.10. SR 3.8.3.2 and SR 3.8.3.5 require verification that the cell float voltages are equal to or greater than the short-term absolute minimum voltage of [2.09] Vpc. The Frequency for cell voltage verification every 31 days for pilot cell and 92 days for each connected cell is consistent with IEEE-450 (Ref. 4). A pilot cell is selected in the series string to reflect the general condition of cells in the battery. The cell selected is the lowest cell voltage in the series string following each quarterly surveillance.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.8.3.3

The limit specified for electrolyte level ensures that the plates suffer no physical damage and maintains adequate electron transfer capability. The Frequency is consistent with IEEE-450 (Ref. 4).

SR 3.8.3.4

COL 16.0-1-A 3.8.3-3

This Surveillance verifies that the required battery pilot cell electrolyte temperature is greater than or equal to the design minimum temperature (i.e., [16°C (60°F)]) to assure the battery can provide the required current and voltage to meet the design requirements. Temperatures lower than assumed in battery sizing calculations reduce battery capacity. The Frequency is consistent with IEEE-450 (Ref. 4).

SR 3.8.3.6

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.

COL 16.0-1-A 3.8.3-4

The acceptance criteria for this Surveillance are consistent with IEEE-450 (Ref. 4) and IEEE-485 (Ref. 5). These references recommend that the battery be replaced if its capacity is below 80% of the manufacturer's rating. A capacity of 80% shows that the battery rate of deterioration is increasing, even if there is ample capacity to meet the load requirements. The battery is sized to meet the assumed duty cycle loads when the battery design capacity reaches this [80]% limit.

The Surveillance Frequency for this test is normally 60 months. If the battery shows degradation, or if the battery has reached 85% of its expected life and capacity is < 100% of the manufacturer's rating, the Surveillance Frequency is reduced to 12 months. However, if the battery shows no degradation but has reached 85% of its expected life, the Surveillance Frequency is only reduced to 24 months for batteries that retain capacity ≥ 100% of the manufacturer's rating. Degradation is indicated, according to IEEE-450 (Ref. 4), when the battery capacity drops by more than 10% relative to its capacity on the previous

BASES

SURVEILLANCE REQUIREMENTS (continued)

performance test or when it is 90% of the manufacturer's rating. All these Frequencies are consistent with the recommendations in IEEE-450 (Ref. 4).

REFERENCES

1. Chapter 8.
2. Chapter 6.
3. Chapter 15.
4. IEEE Standard 450.
5. IEEE Standard 485.

B 3.8 ELECTRICAL POWER SYSTEMS

B 3.8.4 Inverters - Operating

BASES

BACKGROUND

The DC-to-AC inverters are the preferred source of power for the Uninterruptible 120 VAC Power during all modes of operation because of the stability and reliability they achieve in being powered from the associated safety-related DC sources. Uninterruptible 120 VAC Power supplies all safety-related loads, including the Safety-Related Distributed Control and Information System (Q-DCIS) and the control power for safety-related systems.

Each of the four divisions of DC and Uninterruptible AC Electrical Power includes two separate DC-to-AC inverters, one associated with each of the DC Sources. Each inverter receives DC power from either the associated safety-related rectifier or the associated 250 VDC bus that is supported by the battery and charger. The output diodes for the battery chargers and safety-related rectifiers isolate the output of each required battery from an associated 480 VAC isolation power center bus that is de-energized or has degraded voltage.

APPLICABLE SAFETY ANALYSES

The initial conditions of design basis transient and accident analyses in Chapter 6, "Engineered Safety Features," (Ref. 1) and Chapter 15, "Safety Analyses," (Ref. 2) assume Engineered Safety Feature (ESF) systems are OPERABLE. The 250 VDC power system provides normal and emergency 250 VDC power to DC-to-AC inverters, which are used to provide Uninterruptible 120 VAC Power during all modes of operation.

Uninterruptible 120 VAC Power supports Q-DCIS and the control power for safety-related systems.

The OPERABILITY of the 250 VDC power is consistent with the initial assumptions of the accident analyses and is based upon meeting the design basis of the unit. This includes maintaining OPERABILITY of the DC-to-AC inverters needed to support the three divisions of Uninterruptible AC Electrical Power Distribution required by LCO 3.8.6, "Distribution Systems – Operating," so that at least two divisions remain OPERABLE during accident conditions in the event of:

BASES

APPLICABLE SAFETY ANALYSES (continued)

a. An assumed loss of all offsite AC electrical power and all onsite AC electrical power; and

b. A worst-case single failure.

Inverters are a part of the distribution system and, as such, satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

Inverters are required to be OPERABLE to support the three Divisions of DC and Uninterruptible AC Electrical Power Distribution required by LCO 3.8.6, "Distribution Systems – Operating." Each required division is required to have two inverters, one associated with each DC source. An OPERABLE inverter must be connected to the associated Uninterruptible 120 VAC Power bus and maintaining output voltage and frequency within design tolerances.

APPLICABILITY

The inverters are required to be OPERABLE in MODES 1, 2, 3, and 4 to ensure that:

a. Acceptable fuel design limits and reactor coolant pressure boundary limits are not exceeded as a result of AOOs or abnormal transients; and

b. Adequate core cooling is provided, and containment OPERABILITY and other vital functions are maintained in the event of a postulated DBA.

Inverter requirements for MODES 5 and 6 are covered in the Bases for LCO 3.8.5, "Inverters – Shutdown."

ACTIONS

A.1

Condition A represents one inverter inoperable on one required division. In this Condition, the affected division with one inverter remaining OPERABLE can continue to support the immediate safety-related function following a transient event or DBA concurrent with a loss of offsite and onsite AC power, however, it may not have adequate capacity to support the associated division of the Uninterruptible AC Electrical Power Distribution system for the required duration of 72 hours.

BASES

ACTIONS (continued)

With one inverter inoperable on one required division, the Uninterruptible AC Electrical Power Distribution buses in the remaining required divisions are capable of supporting the minimum safety functions necessary to shut down the reactor and maintain it in a safe shutdown condition even with an additional single failure, albeit for less than the design basis 72 hours. In this condition, continued power operation should not exceed 72 hours.

The 72-hour limit is based upon engineering judgment, taking into consideration the time required to repair an inverter and the additional risk to which the plant is exposed because of the inverter inoperability. This risk has to be balanced against the risk of an immediate shutdown, along with the potential challenges to safety systems that such a shutdown might entail.

<u>B.1</u>

Condition B represents two inverters inoperable on one required division. In this Condition, power to the associated Uninterruptible AC Electrical Power Distribution buses cannot be assured following a transient event or DBA concurrent with a loss of offsite and onsite AC power. With both inverters inoperable on one required division, the Uninterruptible AC Electrical Power Distribution buses in the two remaining required divisions are capable of supporting the minimum safety functions necessary to shut down the reactor and maintain it in a safe shutdown condition.

The 8-hour Completion Time for the restoration of an inoperable inverter on one Uninterruptible AC Electrical Power Distribution bus is consistent with the time allowed for an inoperable division of Uninterruptible AC Electrical Power Distribution buses.

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

When one or both inverters on two or more required divisions are inoperable, the remaining inverters may not have the capacity to support a safe shutdown and to mitigate an accident condition, especially if power is lost to the supporting isolation power center buses. If the Required Actions for restoration of a required inverter cannot be met within the specified Completion Time, the plant remains vulnerable to a single failure that could impair the capability to reach safe shutdown or to mitigate an accident condition. Therefore, the unit must be placed

BASES

ACTIONS (continued)

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 12 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 3.8.4.1

This Surveillance verifies that the inverters are functioning properly with all required circuit breakers closed and Uninterruptible AC Electrical Power Distribution buses energized from the inverter. The verification of proper voltage and frequency output ensures that the required power is readily available for Q-DCIS and the control power for safety-related systems connected to the Uninterruptible AC Buses. The 7-day Frequency takes into account the availability of redundant inverters and other indications available in the control room that will alert the operator to inverter malfunctions.

REFERENCES

1. Chapter 6.
2. Chapter 15.

B 3.8 ELECTRICAL POWER SYSTEMS

B 3.8.5 Inverters - Shutdown

BASES

BACKGROUND

A description of the inverters is provided in the Bases for Specification 3.8.4, "Inverters - Operating."

APPLICABLE SAFETY ANALYSES

The initial conditions of design basis transient and accident analyses in Chapter 6, "Engineered Safety Features," (Ref. 1) and Chapter 15, "Safety Analyses," (Ref. 2) assume Engineered Safety Feature (ESF) systems are OPERABLE. The 250 VDC power system provides normal and emergency 250 VDC power to DC-to-AC inverters, which are used to provide Uninterruptible 120 VAC Power during all modes of operation. Uninterruptible 120 VAC Power supports Safety-Related Distributed Control and Information System (Q-DCIS) and the control power for safety-related systems.

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 inverters during MODES 5 and 6 ensures that:

a. The facility can be maintained in the shutdown or refueling condition for extended periods;

b. Sufficient instrumentation and control capability are available for monitoring and maintaining the unit status; and

c. Adequate power is available to mitigate events postulated during shutdown, such as an inadvertent draindown of the vessel.

In general, when the unit is shut down, the Technical Specifications requirements ensure that the unit has the capability to mitigate the consequences of postulated accidents. However, assuming a single failure and concurrent loss of all offsite or all onsite power is not required. The rationale for this is based on the fact that many Design Basis Accidents (DBAs) that are analyzed in MODES 1, 2, 3, and 4 have no specific analyses in MODES 5 and 6. Worst case bounding events are deemed not credible in MODES 5 and 6 because the energy contained within the reactor pressure boundary, reactor coolant temperature and pressure, and the corresponding stresses result in the probabilities of

BASES

APPLICABLE SAFETY ANALYSES (continued)

occurrence being significantly reduced or eliminated, and in minimal consequences. These deviations from DBA analysis assumptions and design requirements during shutdown conditions are allowed by the LCO for required systems.

The shutdown Technical Specification requirements are designed to ensure that the unit has the capability to mitigate the consequences of certain postulated accidents. Worst case DBAs, which are analyzed for operating MODES, are generally viewed not to be a significant concern during shutdown MODES due to the lower energies involved. The Technical Specifications therefore require a lesser complement of electrical equipment to be available during shutdown than is required during operating MODES. More recent work completed on the potential risks associated with shutdown, however, has found significant risk associated with certain shutdown evolutions. As a result, in addition to the requirements established in the Technical Specifications, the industry has adopted NUMARC 91-06, "Guidelines for Industry Actions to Assess Shutdown Management," as an Industry initiative to manage shutdown tasks and associated electrical support to maintain risk at an acceptable low level. This may require the availability of additional equipment beyond that required by the shutdown Technical Specifications.

The inverters are considered part of the Distribution System, and as such, satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

Inverters are required to be OPERABLE to support the Uninterruptible AC Electrical Power Distribution Divisions required by LCO 3.8.7, "Distribution Systems – Shutdown." This LCO ensures the availability of sufficient inverters to operate the unit in a safe manner and to mitigate the consequences of postulated events during shutdown (e.g., inadvertent reactor vessel draindown).

An OPERABLE inverter must be connected to the associated Uninterruptible 120 VAC Power bus and maintaining output voltage and frequency within design tolerances.

BASES

APPLICABILITY	The inverters required to be OPERABLE in MODES 5 and 6 provide assurance that: a. Required features to provide adequate coolant inventory makeup are available for the irradiated fuel assemblies in the core in case of an inadvertent draindown of the reactor vessel; b. Required features necessary to mitigate the effects of events that can lead to core damage during shutdown are available; and c. Instrumentation and control capability is available for monitoring and maintaining the unit in a cold shutdown condition or refueling condition. Inverter requirements for MODES 1, 2, 3, and 4 are covered in LCO 3.8.4, "Inverters - Operating."
ACTIONS	<u>A.1</u> In this Condition, the affected division with one inverter remaining OPERABLE can continue to support the immediate safety-related function following a transient event or DBA concurrent with a loss of offsite and onsite AC power, however, it may not have adequate capacity to support the associated division of the Uninterruptible AC Electrical Power Distribution system for the required duration of 72 hours. With one inverter inoperable on one required division, the Uninterruptible AC Electrical Power Distribution buses in the remaining required divisions are capable of supporting the minimum safety functions necessary to shut down the reactor and maintain it in a safe shutdown condition even with an additional single failure, albeit for less than the design basis 72 hours. The 72 hour limit is based upon engineering judgment, taking into consideration the time required to repair an inverter and the additional risk to which the plant is exposed because of the inverter inoperability. <u>B.1, B.2.1, B.2.2, and B.2.3</u> If two or more required inverters are inoperable, or if the Required Actions for restoration cannot be met within the specified Completion Times, the remaining OPERABLE inverters may be capable of supporting sufficient required feature(s) to allow continuation of CORE ALTERATIONS and operations with a potential for draining the reactor vessel. By allowing

BASES

ACTIONS (continued)

the option to declare required feature(s) associated with an inoperable inverter inoperable, appropriate restrictions are implemented in accordance with the affected required feature(s) of the LCOs' ACTIONS. In many instances this option may involve undesired administrative efforts. Therefore, the allowance for sufficiently conservative actions is made (i.e., to suspend CORE ALTERATIONS and any activities that could potentially result in inadvertent draining of the reactor vessel).

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 plant safety-related 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's safety-related systems may be without power.

SURVEILLANCE REQUIREMENTS

SR 3.8.5.1

This Surveillance verifies that the inverters are functioning properly with all required circuit breakers closed and Uninterruptible AC Electrical Power Distribution buses energized from the inverter. The verification of proper voltage and frequency output ensures that the required power is readily available for the Q-DCIS and the control power for safety-related systems connected to the Uninterruptible AC Electrical Power Distribution buses. The 7-day Frequency takes into account the redundant capability of the inverters and other indications available in the control room that will alert the operator to inverter malfunctions.

REFERENCES

1. Chapter 6.
2. Chapter 15.

B 3.8 ELECTRICAL POWER SYSTEMS

B 3.8.6 Distribution Systems - Operating

BASES

BACKGROUND

The DC Electrical Power Distribution system provides the normal and emergency power to the DC-to-AC inverters, which are used to provide Uninterruptible 120 VAC Power during all modes of operation. Uninterruptible 120 VAC Power supplies all safety-related loads, including the Safety-Related Distributed Control and Information System (Q-DCIS) and the control power for safety-related systems. The DC and Uninterruptible 120 VAC Electrical Power Distribution system is designed to have sufficient capacity, independence, redundancy, and testability to perform its safety functions, assuming a single failure, when any three of the four divisions are available.

Each of the four divisions of DC and Uninterruptible AC Electrical Power distribution includes two 250 VDC Electrical Power Distribution buses and two Uninterruptible 120 VAC Power buses.

Each of the two 250 VDC Electrical Power Distribution buses in each division is powered from an associated DC source consisting of a battery and a battery charger that is powered from an isolation power center bus. The output of each 250 VDC Electrical Power Distribution bus is the safety-related and uninterruptible source of power to an associated DC-to-AC inverter. A safety-related rectifier powered from the isolation power center bus provides the normal source of power to the inverter. If there is loss of power to the isolation power center bus or the safety-related rectifier fails, the 250 VDC Electrical Power Distribution bus will transparently continue to supply power to the Inverter. The Bases for Specification 3.8.1, "DC Sources - Operating," provides a more detailed description of the DC Sources and the 250 VDC Electrical Power Distribution buses.

The two inverters in each safety-related division are configured for parallel redundant operation to allow load sharing and the equal discharge of the division’s safety-related batteries to the Uninterruptible 120 VAC Electrical Power buses in each division. The inverter, which receives its power from a 250 VDC Electrical Power Distribution bus as described above, is the safety-related, uninterruptible source of power to an associated Uninterruptible 120 VAC Electrical Power bus.

BASES

BACKGROUND (continued)

The Bases for Specification 3.8.4, "Inverters - Operating," provides a more detailed description of the inverters and the Uninterruptible 120 VAC Electrical Power buses.

The DC and Uninterruptible AC Electrical Power Distribution buses are listed in Table B 3.8.6-1. Two divisions (1 and 2) of safety-related power supply the reactor protection system (RPS) scram pilot valve solenoids and the same two divisions supply power to the main steam isolation valve (MSIV) solenoids.

APPLICABLE SAFETY ANALYSES

The initial conditions of design basis transient and accident analyses in Chapter 6, "Engineered Safety Features," (Ref. 1) and Chapter 15, "Safety Analyses," (Ref. 2) assume Engineered Safety Feature (ESF) systems are OPERABLE. The DC Electrical Power Distribution system provides the normal and emergency power to the DC-to-AC inverters, which are used to provide Uninterruptible 120 VAC Power during all modes of operation. Uninterruptible 120 VAC Power supplies all safety-related loads, including the Q-DCIS and the control power for safety-related systems.

The OPERABILITY of the DC and Uninterruptible AC Electrical Power Distribution is consistent with the initial assumptions of the accident analyses and is based upon meeting the design basis of the unit. This includes maintaining OPERABILITY of three divisions of Uninterruptible AC Electrical Power so that at least two divisions remain OPERABLE during accident conditions in the event of:

a. An assumed loss of all offsite AC electrical power and all onsite AC electrical power; and

b. A worst-case single failure.

The DC and Uninterruptible AC Electrical Power Distribution system satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

Three of the four divisions of DC and Uninterruptible AC Electrical Power Distribution buses listed in Table B 3.8.6-1 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 Design Basis Accident (DBA).

BASES

LCO (continued)

Maintaining any three of the four divisions of DC and Uninterruptible AC Electrical Power Distribution buses OPERABLE ensures that the redundancy incorporated into the design of ESF is not defeated. Any two of the four divisions of the distribution system are capable of providing the necessary electrical power to the associated ESF components. Therefore, a single failure within any system or within the electrical power distribution does not prevent safe shutdown of the reactor.

OPERABLE 250 VDC Electrical Power Distribution buses must be energized to their proper voltage from either the associated battery or charger. OPERABLE Uninterruptible 120 VAC Electrical Power buses must be energized to their proper voltage and frequency.

APPLICABILITY

The electrical power distribution subsystems are required to be OPERABLE in MODES 1, 2, 3, and 4 to ensure that:

a. Acceptable fuel design limits and reactor coolant pressure boundary limits are not exceeded as a result of AOOs or abnormal transients; and

b. Adequate core cooling is provided, and containment OPERABILITY and other vital functions are maintained in the event of a postulated DBA.

Electrical power distribution subsystem requirements for MODES 5 and 6 are covered in the Bases for LCO 3.8.7, "Distribution Systems – Shutdown."

ACTIONS

A.1

Condition A represents one 250 VDC Electrical Power Distribution bus in one required division inoperable. In this Condition, the remaining OPERABLE 250 VDC Electrical Power Distribution bus in the associated division can continue to support the immediate safety-related function following a transient event or DBA concurrent with a loss of offsite and onsite AC power.

BASES

ACTIONS (continued)

With one 250 VDC Electrical Power Distribution bus inoperable in one required division, the remaining required divisions of DC and Uninterruptible AC Electrical Power have the capacity to support a safe shutdown and to mitigate an accident condition even with an additional single failure, and even if power is lost to the supporting isolation power center buses, albeit for less than the design basis 72 hours. The 72-hour Completion Time for restoration is based upon engineering judgment.

<u>B.1</u>

Condition B represents both 250 VDC Electrical Power Distribution buses in one required division inoperable. In this Condition, power to the associated Uninterruptible AC Electrical Power Distribution buses cannot be assured during an event that includes loss of power to the associated isolation power center bus, which supplies power to the battery chargers and the safety-related rectifiers.

With both 250 VDC Electrical Power Distribution buses inoperable in one required division, the two remaining required divisions of DC and Uninterruptible AC Electrical Power have the capacity to support a safe shutdown and to mitigate an accident condition even if power is lost to the supporting isolation power center buses. Since a subsequent worst-case single failure could, however, result in the loss of minimum necessary DC electrical subsystems, continued power operation should not exceed 8 hours. The 8-hour Completion Time for restoration is based upon engineering judgment.

<u>C.1</u>

Condition C represents one Uninterruptible 120 VAC Electrical Power bus inoperable in one required division. In this Condition, the remaining OPERABLE Uninterruptible 120 VAC Electrical Power Distribution bus in the associated division can continue to support the immediate safety-related function following a transient event or DBA concurrent with a loss of offsite and onsite AC power. The remaining divisions with OPERABLE Uninterruptible 120 VAC Electrical Power buses still have the capacity to support a safe shutdown and to mitigate an accident condition even with an additional single failure, and even if power is lost to the supporting isolation power center buses, albeit for less than the design basis 72 hours. The 72-hour Completion Time is based on engineering judgment.

BASES

ACTIONS (continued)

D.1

Condition D represents both Uninterruptible 120 VAC Electrical Power buses inoperable in one required division. In this condition, the voltage and frequency of the power being supplied to the safety-related loads for that division, including the Q-DCIS and the control power for safety-related systems, cannot be maintained within required limits even when the associated isolation power center bus remains energized. The two remaining divisions with OPERABLE 120 VAC Electrical Power buses still have the capacity to support a safe shutdown and to mitigate an accident condition even if power is lost to the supporting isolation power center buses. Since a subsequent single failure could, however, result in the loss of minimum necessary Uninterruptible 120 VAC Electrical Power buses, continued power operation should not exceed 8 hours. The 8-hour Completion Time is based on engineering judgment.

E.1 and E.2

Condition E represents inoperability of one Uninterruptible AC Electrical Power Distribution bus on one required division concurrent with inoperability of the DC Electrical Power Distribution bus associated with the redundant AC Electrical Power Distribution bus on the same division. With the inoperability of the DC Electrical Power Distribution bus, power to the associated Uninterruptible AC Electrical Power Distribution bus cannot be assured during an event that includes loss of power to the associated isolation power center bus. Therefore, in this condition, the required division is not able to support the immediate safety-related function following a transient event or DBA concurrent with a loss of offsite and onsite AC power. The two remaining required divisions of DC and Uninterruptible AC Electrical Power have the capacity to support a safe shutdown and to mitigate an accident condition even if power is lost to the supporting isolation power center buses. Since a subsequent worst-case single failure could, however, result in the loss of minimum necessary DC electrical subsystems, continued power operation should not exceed 8 hours. The 8-hour Completion Time for restoration is based upon engineering judgment.

BASES

ACTIONS (continued)

F.1 and F.2

Condition F represents two or more required divisions with one or more DC or Uninterruptible AC Electrical Power Distribution buses (i.e., any combination) inoperable, or the Required Action and associated Completion Time of Condition A, B, C, D, or Enot met. When one or more DC or Uninterruptible AC Electrical Power Distribution buses (i.e., any combination) on two or more required divisions are inoperable, the remaining Electrical Power Distribution buses may not have the capacity to support a safe shutdown and to mitigate an accident condition. If the Required Actions for restoration of a required DC or Uninterruptible AC Electrical Power Distribution bus cannot be met within the specified Completion Time, the plant remains vulnerable to a single failure that could impair the capability to reach safe shutdown or to mitigate an accident condition. Therefore, the unit must be placed in a MODE that minimizes risk. To achieve this status, the plant must be brought to at least MODE 3 within 12 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 3.8.6.1

This Surveillance verifies that the DC and Uninterruptible AC Electrical Power Distribution buses are functioning properly, with the correct circuit breaker alignment and that the buses energized from normal power. The correct breaker alignment ensures the appropriate voltage is available to each required bus. The verification of proper voltage availability on the buses ensures that the required power is readily available for all safety-related loads, including the Q-DCIS and the control power for safety-related systems. The 7-day Frequency takes into account the redundant capability of the DC and Uninterruptible AC Electrical Power Distribution buses, and other indications available in the control room that will alert the operator to subsystem malfunctions.

REFERENCES

1. Chapter 6.
2. Chapter 15.

Table B 3.8.6-1 (page 1 of 1)
DC and Uninterruptible AC Electrical Power Distribution

TYPE	VOLTAGE	DIVISION 1	DIVISION 2	DIVISION 3	DIVISION 4
Electrical Power Distribution buses	250 VDC	Bus 11 Bus 12	Bus 21 Bus 22	Bus 31 Bus 32	Bus 41 Bus 42
Uninterruptible Electrical Power buses	120 VAC	Bus 11 Bus 12	Bus 21 Bus 22	Bus 31 Bus 32	Bus 41 Bus 42

B 3.8 ELECTRICAL POWER SYSTEMS

B 3.8.7 Distribution Systems - Shutdown

BASES

BACKGROUND	A description of DC and Uninterruptible AC Electrical Power Distribution is provided in the Bases for LCO 3.8.6, "Distribution System - Operating."

APPLICABLE SAFETY ANALYSES

The initial conditions of design basis transient and accident analyses in Chapter 6, "Engineered Safety Features," (Ref. 1) and Chapter 15, "Safety Analyses," (Ref. 2) assume Engineered Safety Feature (ESF) systems are OPERABLE. The DC electrical power system provides normal and emergency DC electrical power to DC-to-AC inverters, which are used to provide Uninterruptible 120 VAC Power during all modes of operation. Uninterruptible 120 VAC Power supports Safety-Related Distributed Control and Information System (Q-DCIS) and the control power for safety-related systems.

The OPERABILITY of DC and Uninterruptible AC Electrical Power Distribution is consistent with the initial assumptions of the accident analyses and the requirements for the supported systems' OPERABILITY. The OPERABILITY of DC and Uninterruptible AC Electrical Power Distribution during MODES 5 and 6 ensures that:

a. The facility can be maintained in the shutdown or refueling condition for extended periods,

b. Sufficient instrumentation and control capability is available for monitoring and maintaining the unit status, and

c. Adequate power is provided to mitigate events postulated during shutdown, such as an inadvertent draindown of the vessel.

In general, when the unit is shut down, the Technical Specifications requirements ensure that the unit has the capability to mitigate the consequences of postulated accidents. However, assuming a single failure and concurrent loss of all offsite or all onsite power is not required. The rationale for this is based on the fact that many Design Basis Accidents (DBAs) that are analyzed in MODES 1, 2, 3, and 4 have no specific analyses in MODES 5 and 6. Worst case bounding events are

BASES

APPLICABLE SAFETY ANALYSES (continued)

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.

The shutdown Technical Specification requirements are designed to ensure that the unit has the capability to mitigate the consequences of certain postulated accidents. Worst case DBAs, which are analyzed for operating MODES, are generally viewed not to be a significant concern during shutdown MODES due to the lower energies involved. The Technical Specifications therefore require a lesser complement of electrical equipment to be available during shutdown than is required during operating MODES. More recent work completed on the potential risks associated with shutdown, however, has found significant risk associated with certain shutdown evolutions. As a result, in addition to the requirements established in the Technical Specifications, the industry has adopted NUMARC 91-06, "Guidelines for Industry Actions to Assess Shutdown Management," as an Industry initiative to manage shutdown tasks and associated electrical support to maintain risk at an acceptable low level. This may require the availability of additional equipment beyond that required by the shutdown Technical Specifications.

DC and Uninterruptible AC Electrical Power Distribution satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

DC and Uninterruptible AC Electrical Power Distribution buses are required to be OPERABLE to support equipment required to respond to any anticipated operational occurrence (AOO) or DBA. Various LCOs establish requirements for a minimum number of divisions, subsystems, or trains of equipment needed to respond to an AOO or DBA depending on the specific plant 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 Technical Specifications' required divisions, subsystems, or trains - both specifically addressed by their own LCOs and implicitly required by the definition of OPERABILITY.

BASES

LCO (continued)

Maintaining these portions of DC and Uninterruptible AC Electrical Power Distribution energized ensures the availability of sufficient power to operate the plant in a safe manner to mitigate the consequences of postulated events during shutdown (e.g., inadvertent reactor vessel draindown).

APPLICABILITY

The DC and Uninterruptible AC Electrical Power Distribution is required to be OPERABLE in MODES 5 and 6 to provide assurance that:

a. Systems to provide adequate coolant inventory makeup are available for the irradiated fuel in the core in case of an inadvertent draindown of the reactor vessel;

b. Required features necessary to mitigate the effects of events that can lead to core damage during shutdown are available; and

c. Instrumentation and control capability is available for monitoring and maintaining the unit in a cold shutdown condition or refueling condition.

DC and Uninterruptible AC electrical power distribution subsystem requirements for MODES 1, 2, 3, and 4 are covered in LCO 3.8.6, "Distribution Systems - Operating."

ACTIONS

A.1

Condition A represents one 250 VDC Electrical Power Distribution bus in one required division inoperable. In this Condition, the remaining OPERABLE 250 VDC Electrical Power Distribution bus in the associated division can continue to support the immediate safety-related function following a transient event or DBA concurrent with a loss of offsite and onsite AC power.

With one 250 VDC Electrical Power Distribution bus inoperable in one required division, the remaining required divisions of DC Electrical Power buses have the capacity to support a safe shutdown and to mitigate an accident condition even with an additional single failure, and even if power is lost to the supporting isolation power center buses, albeit for less than the design basis 72 hours. The 72 hour Completion Time for restoration is based upon engineering judgment.

ACTIONS (continued)

B.1

Condition B represents one Uninterruptible 120 VAC Electrical Power Distribution bus inoperable in one required division. In this Condition, the remaining OPERABLE Uninterruptible 120 VAC Electrical Power Distribution bus in the associated division can continue to support the immediate safety-related function following a transient event or DBA concurrent with a loss of offsite and onsite AC power. The remaining divisions with OPERABLE Uninterruptible 120 VAC Electrical Power buses still have the capacity to support a safe shutdown and to mitigate an accident condition even with an additional single failure, and even if power is lost to the supporting isolation power center buses. The 72 hour Completion Time is based on engineering judgment.

C.1, C.2.1, C.2.2 and C.2.3

If two or more required 250 VDC Electrical Power Distribution buses are inoperable, or two or more required Uninterruptible 120 VAC Electrical Power Distribution buses are inoperable, or one 120 VAC Electrical Power Distribution bus on one required division is inoperable concurrent with the 250 VDC Electrical Power Distribution bus associated with the redundant AC Electrical Power Distribution bus on the same division being inoperable, or if the Required Actions for restoration cannot be met within the specified Completion Times, the remaining OPERABLE electrical power distribution Division may be capable of supporting sufficient required features to allow continuation of CORE ALTERATIONS and operations with a potential for draining the reactor vessel. By allowing the option to declare required features associated with an inoperable distribution subsystem inoperable, appropriate restrictions are implemented in accordance with the affected distribution subsystem LCO's Required Actions. In many instances this option may involve undesired administrative efforts. Therefore, the allowance for sufficiently conservative actions is made (i.e., to suspend CORE ALTERATIONS and any activities that could potentially result in inadvertent draining of the reactor vessel).

Suspension of these activities shall not preclude completion of actions to establish a safe conservative condition. These actions will minimize probability of the occurrence of postulated events. It is further required to

BASES

ACTIONS (continued)

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's safety-related systems.

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's safety-related systems may be without power.

SURVEILLANCE REQUIREMENTS

SR 3.8.7.1

This Surveillance verifies that the DC and Uninterruptible AC Electrical Power Distribution systems are functioning properly, with the required 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, as well as other indications available in the control room that will alert the operator to subsystem malfunctions.

REFERENCES

1. Chapter 6.
2. Chapter 15.

B 3.9 REFUELING OPERATIONS

B 3.9.1 Refueling Equipment Interlocks

BASES

BACKGROUND

Refueling equipment interlocks restrict the operation of the refueling equipment or the withdrawal of control rods to reinforce plant procedures in preventing the reactor from achieving criticality during refueling. The refueling interlock circuitry senses the conditions of the refueling equipment and the control rods. Depending on the sensed conditions, interlocks are actuated to prevent the operation of the refueling equipment or the withdrawal of control rods.

GDC 26 of 10 CFR 50, Appendix A, requires that one of the two required independent reactivity control systems be capable of holding the reactor core subcritical under cold conditions (Ref. 1). The control rods, when fully inserted, serve as the system capable of maintaining the reactor subcritical in cold conditions during all fuel movement activities and accidents.

Two channels of instrumentation are provided to sense the full insertion of control rods, the position of the refueling machine, and the loading of the refueling machine fuel grapple or auxiliary hoist. With the reactor mode switch in the refueling position, the indicated conditions are combined in logic circuits to determine if all restrictions on refueling equipment operations and control rod insertion are satisfied.

A control rod not at its full-in position interrupts power to the refueling equipment and prevents operating the equipment over the reactor core when loaded with a fuel assembly. Conversely, the refueling equipment located over the core and loaded with fuel generates a control rod withdrawal block signal in the Rod Control & Information System to prevent withdrawing a control rod.

The refueling interlocks prevent operation of the refueling equipment with fuel loaded over the core whenever any control rod is withdrawn, or to prevent control rod withdrawal whenever fuel-loaded refueling equipment is over the core (Ref. 2).

BASES

APPLICABLE SAFETY ANALYSES	The refueling interlocks are explicitly assumed in the safety analysis of the control rod removal error during refueling (Ref. 3). This analysis evaluates the consequences of control rod withdrawal during refueling. A prompt reactivity excursion during refueling could potentially result in fuel failure with subsequent release of radioactive material to the environment. Criticality and, therefore, subsequent prompt reactivity excursions are prevented during the insertion of fuel, provided all control rods are fully inserted during the fuel insertion. The refueling interlocks accomplish this by preventing loading fuel into the core with any control rod withdrawn, or by preventing withdrawal of a rod from the core during fuel loading. Refueling Equipment Interlocks satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).
LCO	To prevent criticality during refueling, the refueling interlocks associated with the reactor mode switch in Refuel position ensure that fuel assemblies are not loaded into the core with any control rod withdrawn. To prevent these conditions from developing, the all-rods-in, the refueling machine position, and the refueling machine fuel grapple hoist fuel-loaded (or auxiliary hoist fuel-loaded, if being used) inputs are required to be OPERABLE. These inputs are combined in logic circuits that provide refueling equipment or control rod blocks to prevent operations that could result in criticality during refueling operations.
APPLICABILITY	In MODE 6, a prompt reactivity excursion could cause fuel damage and subsequent release of radioactive material to the environment. The refueling equipment interlocks protect against prompt reactivity excursions during MODE 6. The interlocks are only required to be OPERABLE during in-vessel fuel movement with refueling equipment associated with the interlocks when the reactor mode switch is in the Refuel position.

BASES

APPLICABILITY (continued)

When the reactor mode switch is in the Shutdown position, a control rod block (LCO 3.3.2.1, "Control Rod Block Instrumentation") ensures control rod withdrawal cannot occur simultaneously with in-vessel fuel movement. In MODES 1, 2, 3, 4, and 5, the reactor pressure vessel (RPV) head is on and no fuel loading activities are possible. Therefore, the refueling interlocks are not required to be OPERABLE in these conditions.

ACTIONS

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

With one or more of the required refueling equipment interlocks inoperable, the plant must be placed in a condition in which the LCO does not apply. Therefore, Required Action A.1 requires that in-vessel fuel movement with the affected refueling equipment must be immediately suspended. This action ensures that operations are not performed with equipment that would potentially not be blocked from unacceptable operations (e.g., loading fuel into a cell with a control rod withdrawn). Suspension of in-vessel fuel movement shall not preclude completion of movement of a component to a safe position.

Alternatively, Required Actions A.2.1 and A.2.2 require a control rod withdrawal block to be inserted, and all control rods to be subsequently verified to be fully inserted. Required Action A.2.1 ensures no control rods can be withdrawn, because a block to control rod withdrawal is in place. The withdrawal block utilized must ensure that if rod withdrawal is requested, the rod will not respond (i.e., it will remain inserted). Required Action A.2.2 is performed after placing the rod withdrawal block in effect, and provides a verification that all control rods are fully inserted. This verification that all control rods are fully inserted is in addition to the periodic verifications required by SR 3.9.3.1.

Like Required Action A.1, Required Actions A.2.1 and A.2.2 ensure unacceptable operations are blocked (e.g., loading fuel into a cell with the control rod withdrawn).

BASES

SURVEILLANCE REQUIREMENTS	SR 3.9.1.1 Performance of a CHANNEL FUNCTIONAL TEST demonstrates each required refueling equipment interlock will function properly when a simulated or actual signal indicative of a required condition is injected into the logic. The CHANNEL FUNCTIONAL TEST may be performed by any series of sequential, overlapping, or total channel steps such that the entire channel is tested. The 7-day Frequency is based on engineering judgment and is considered adequate in view of other indications of refueling interlocks and their associated input status that are available to plant operations personnel.
REFERENCES	1. 10 CFR 50, Appendix A, GDC 26. 2. Section 7.7.2. 3. Section 15.3.7.

B 3.9 REFUELING OPERATIONS

B 3.9.2 Refuel Position One-Rod/Rod-Pair-Out Interlock

BASES

BACKGROUND

The refuel position one-rod/rod-pair-out interlock restricts the movement of control rods to reinforce plant procedures that prevent the reactor from becoming critical during refueling operations. During refueling operations, no more than one control rod or control rod pair with the same hydraulic control unit (HCU) is permitted to be withdrawn. To enable the one-rod/rod-pair-out interlock, the Rod Control and Information System (RC&IS) GANG/SINGLE selection switch may be in "SINGLE" or "GANG" mode. Otherwise, it is not possible to withdraw the one or two rods associated with the same HCU, respectively, while in the refueling mode.

GDC 26 of 10 CFR 50, Appendix A, requires that one of the two required independent reactivity control systems be capable of holding the reactor core subcritical under cold conditions (Ref. 1). The control rods serve as the system capable of maintaining the reactor subcritical in cold conditions.

The refuel position one-rod/rod-pair-out interlock prevents the selection of a second control rod for movement when any other control rod or control rod pair is not fully inserted (Ref. 2). It is a logic circuit, which has redundant channels. It uses the all-rods-in signal (from the control rod full-in position indicators discussed in LCO 3.9.4, "Control Rod Position Indication") and a rod selection signal (from the RC&IS).

APPLICABLE SAFETY ANALYSES

The refuel position one-rod/rod-pair-out interlock is explicitly assumed in the safety analysis of the control rod withdrawal error during refueling (Ref. 3). This analysis evaluates the consequences of control rod withdrawal during refueling. A prompt reactivity excursion during refueling could potentially result in fuel failure with subsequent release of radioactive material to the environment.

The refuel position one-rod/rod-pair-out interlock and adequate SDM (LCO 3.1.1, "SHUTDOWN MARGIN") prevent criticality by preventing withdrawal of more than one control rod or control rod pair. With one control rod or control rod pair withdrawn, the core will remain subcritical, thereby preventing any prompt critical excursion.

BASES

APPLICABLE SAFETY ANALYSES (continued)

The refuel position one-rod/rod-pair-out Interlock satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

To prevent criticality during MODE 6, the refuel position one-rod/rod-pair-out interlock ensures no more than one control rod or one control rod pair with the same HCU may be withdrawn. The refuel position one-rod/rod-pair-out interlock is required to be OPERABLE and the reactor mode switch must be locked in the refuel position to support the OPERABILITY of the interlock.

APPLICABILITY

In MODE 6, with the reactor mode switch in the refuel position, the OPERABLE refuel position one-rod/rod-pair-out interlock provides protection against prompt reactivity excursions.

In MODES 1, 2, 3, 4 and 5, the refuel position one-rod/rod-pair-out interlock is not required to be OPERABLE and is bypassed. In MODES 1 and 2, the Reactor Protection System (RPS) (LCO 3.3.1.1, "Reactor Protection System (RPS) Instrumentation," LCO 3.3.1.2, "Reactor Protection System (RPS) Actuation," and LCO 3.3.1.3, "Reactor Protection System (RPS) Manual Actuation") and the control rods (LCO 3.1.3, "Control Rod OPERABILITY") provide mitigation of potential reactivity excursions. In MODES 3, 4 and 5, with the reactor mode switch in the shutdown position, a control rod block (LCO 3.3.2.1, "Control Rod Block Instrumentation") ensures all control rods are inserted, thereby preventing criticality during shutdown conditions.

ACTIONS

A.1 and A.2

With the refuel position one-rod/rod-pair-out interlock inoperable, the refueling interlocks may not be capable of preventing more than one control rod or control rod pair from being withdrawn. This condition may lead to criticality.

BASES

ACTIONS (continued)

Control rod withdrawal must be immediately suspended, and action must be immediately initiated to fully insert all insertable control rods in core cells containing one or more fuel assemblies. Action must continue until all such control rods are fully inserted. Control rods in core cells containing no fuel assemblies do not affect the reactivity of the core and, therefore, do not have to be inserted.

SURVEILLANCE REQUIREMENTS

SR 3.9.2.1

Proper functioning of the refuel position one-rod/rod-pair-out interlock requires the reactor mode switch to be in refuel. During control rod withdrawal in MODE 6, improper positioning of the reactor mode switch could, in some instances, allow improper bypassing of required interlocks. Therefore, this Surveillance imposes an additional level of assurance that the refuel position one-rod/rod-pair-out interlock will be OPERABLE when required. By "locking" the reactor mode switch in the proper position (i.e., removing the reactor mode switch key from the console while the reactor mode switch is positioned in refuel), an additional administrative control is in place to preclude operator errors from resulting in unanalyzed operation.

The Frequency of 12 hours is sufficient, in view of other administrative controls utilized during refueling operations, to ensure safe operation.

SR 3.9.2.2

Performance of a CHANNEL FUNCTIONAL TEST on each channel demonstrates the associated refuel position one-rod/rod-pair-out interlock will function properly when a simulated or actual signal indicative of a required condition is injected into the logic. The CHANNEL FUNCTIONAL TEST may be performed by any series of sequential, overlapping, or total channel steps such that the entire channel is tested. The 7-day Frequency is considered adequate because of demonstrated circuit reliability, procedural controls on control rod withdrawals, and visual and audible indications available in the control room to alert the operator of control rods not fully inserted.

BASES

SURVEILLANCE REQUIREMENTS (continued)

To perform the required testing, the applicable condition must be entered (i.e., a control rod must be withdrawn from its full-in position). Therefore, SR 3.9.2.2 has been modified by a Note that states the CHANNEL FUNCTIONAL TEST is only required to be performed within 1 hour after any control rod is withdrawn.

REFERENCES

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

2. Section 7.7.2.

3. Section 15.3.7.

B 3.9 REFUELING OPERATIONS

B 3.9.3 Control Rod Position

BASES

BACKGROUND	Control rods provide the capability to maintain the reactor subcritical under all conditions and to limit the potential amount and rate of reactivity increase caused by a malfunction in the Control Rod Drive (CRD) System. During refueling, movement of control rods is limited by the refueling interlocks (LCO 3.9.1, "Refueling Equipment Interlocks" and LCO 3.9.2, "Refuel Position One-Rod/Rod-Pair-Out Interlock") or the control rod block with the reactor mode switch in the shutdown position (LCO 3.3.2.1, "Control Rod Block Instrumentation"). GDC 26 of 10 CFR 50, Appendix A, requires that one of the two required independent reactivity control systems be capable of holding the reactor core subcritical under cold conditions (Ref. 1). The control rods serve as the system capable of maintaining the reactor subcritical in cold conditions. When the Rod Control and Information System (RC&IS) GANG/SINGLE selection status is in the SINGLE mode, the refueling interlocks allow a single control rod to be withdrawn at any time unless fuel is being loaded into the core. However, when the RC&IS GANG/SINGLE selection status is in the GANG mode with the individual hydraulic control unit (HCU) scram test mode active, the refueling interlocks allow the one or two control rods that are associated with the same HCU to be withdrawn at any time unless fuel is being loaded into the core. To preclude loading fuel assemblies into the core with a control rod or control rod pair withdrawn, all control rods must be fully inserted. This prevents the reactor from achieving criticality during refueling operations.
APPLICABLE SAFETY ANALYSES	Prevention and mitigation of prompt reactivity excursions during refueling are provided by the refueling interlocks (LCO 3.9.1 and LCO 3.9.2), the SDM (LCO 3.1.1, "SHUTDOWN MARGIN"), the startup range neutron monitor neutron flux scram (LCO 3.3.1.1, "Reactor Protection System (RPS) Instrumentation" and LCO 3.3.1.2, "Reactor Protection System (RPS) Actuation"), and the control rod block instrumentation (LCO 3.3.2.1).

BASES

APPLICABLE SAFETY ANALYSES (continued)

The safety analysis of the control rod removal error during refueling (Ref. 2) assumes the functioning of the refueling interlocks and adequate SDM. Additionally, prior to fuel reload, all control rods must be fully inserted to minimize the probability of an inadvertent criticality.

Control Rod Position satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

All control rods must be fully inserted during applicable refueling conditions to prevent an inadvertent criticality during refueling.

APPLICABILITY

During MODE 6, loading fuel into a core cell with the control rod withdrawn may result in inadvertent criticality. Therefore, the control rod must be inserted before loading fuel into a core cell. All control rods must be inserted before loading fuel to ensure that a fuel loading error does not result in loading fuel into a core cell with the control rod withdrawn.

In MODES 1, 2, 3, 4, and 5, the reactor pressure vessel (RPV) head is on and no fuel loading activities are possible. Therefore, this specification is not applicable in these MODES.

ACTIONS

A.1

With all control rods not fully inserted during the applicable conditions, an inadvertent criticality could occur that is not analyzed. All fuel loading operations must be immediately suspended. Suspension of these activities shall not preclude the completion of movement of a component to a safe condition.

BASES

SURVEILLANCE REQUIREMENTS	SR 3.9.3.1 During refueling, to ensure that the reactor remains subcritical, all control rods must be fully inserted prior to and during fuel loading. Periodic checks of the control rod position ensure this condition is maintained. The 12-hour Frequency considers the procedural controls on control rod movement during refueling as well as the redundant functions of the refueling interlocks.
REFERENCES	1. 10 CFR 50, Appendix A, GDC 26. 2. Section 15.3.7.

B 3.9 REFUELING OPERATIONS

B 3.9.4 Control Rod Position Indication

BASES

BACKGROUND	The full-in position indication channel for each control rod provides information necessary to the refueling interlocks. During refueling, the refueling interlocks (LCO 3.9.1, "Refueling Equipment Interlocks" and LCO 3.9.2, "Refuel Position One-Rod/Rod-Pair-Out Interlock") use the full-in position indication channels to limit the operation of the refueling equipment and the movement of the control rods. The absence of the full-in position indication channel signal for any control rod prevents the refueling platform from being moved over the core if fuel is loaded in the hoist, thereby preventing fuel loading. Also, this condition prevents the withdrawal of any other control rod. GDC 26 of 10 CFR 50, Appendix A, requires that one of the two required independent reactivity control systems be capable of holding the reactor core subcritical under cold conditions (Ref. 1). The control rods serve as the system capable of maintaining the reactor subcritical in cold conditions.
APPLICABLE SAFETY ANALYSES	Prevention and mitigation of prompt reactivity excursions during refueling are provided by the refueling interlocks (LCO 3.9.1 and LCO 3.9.2), the SHUTDOWN MARGIN (LCO 3.1.1), the startup range neutron monitor (SRNM) neutron flux scram (LCO 3.3.1.1, "Reactor Protection System (RPS) Instrumentation" and LCO 3.3.1.2, "Reactor Protection System (RPS) Actuation"), and the control rod block instrumentation (LCO 3.3.2.1, "Control Rod Block Instrumentation"). The safety analysis for the control rod withdrawal error during refueling (Ref. 2) assumes the functioning of the refueling interlocks and adequate SDM. The full-in position indication channel is required to be OPERABLE so that the refueling interlocks can ensure that fuel cannot be loaded with any control rod or control rod pair withdrawn, and that no more than one control rod or control rod pair can be withdrawn at a time. Control Rod Position Indication satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO

Control rod full-in position indication channels must be OPERABLE to provide the required inputs to the refueling interlocks. A channel is OPERABLE if it provides correct position indication to the refueling equipment interlock all-rods-in logic (LCO 3.9.1), and correct position indication to the refuel position one-rod/rod-pair-out interlock logic (LCO 3.9.2).

APPLICABILITY

During MODE 6, the control rods must have OPERABLE full-in position indication to ensure the applicable refueling interlocks will be OPERABLE.

In MODES 1 and 2, requirements for control rod position are specified in LCO 3.1.3, "Control Rod OPERABILITY." In MODES 3, 4, and 5, with the reactor mode switch in the shutdown position, a control rod block (LCO 3.3.2.1), ensures all control rods are inserted, thereby preventing criticality during shutdown conditions.

ACTIONS

A Note has been provided to modify the ACTIONS related to control rod position indication channels. Section 1.3, Completion Times, specifies once a Condition has been entered, subsequent divisions, subsystems, components, or variables expressed in the Condition discovered to be inoperable or not within limits, will not result in separate entry into the Condition. Section 1.3 also specifies Required Actions of the Condition continue to apply for each additional failure, with Completion Times based on initial entry into the Condition. However, the Required Actions for control rods with inoperable position indication channels provide appropriate compensatory measures. As such, a Note has been provided which allows separate Condition entry for each control rod with inoperable position indication channels.

<u>A.1.1, A.1.2, A.1.3, A.2.1, and A.2.2</u>

With one or more required full-in position indication channels inoperable, compensating actions must be taken to protect against potential reactivity excursions from fuel assembly insertions or control rod withdrawals. This may be accomplished by immediately suspending in-vessel fuel movement and control rod withdrawal, and immediately initiating action to fully insert all insertable control rods in core cells containing one or more fuel assemblies. Actions must continue until all insertable control rods in

BASES

ACTIONS (continued)

core cells containing one or more fuel assemblies are fully inserted. Suspension of in-vessel fuel movements and control rod withdrawal shall not preclude completion of the movement of a component to a safe condition.

Alternatively, actions may be immediately initiated to fully insert the control rod(s) associated with the inoperable full-in position indicator(s) and disarm the drive(s) to ensure that the control rod is not withdrawn. Actions must continue until all associated control rods are fully inserted and drives are disarmed. Under these conditions (control rod full inserted and disarmed), an inoperable full-in channel may be bypassed to allow refueling operations to proceed. An alternate method must be used to ensure the control rod is fully inserted (e.g., use the latched full-in and full-in position reed switches). Another option is to bypass Resolver A (which is the current position probe) and use Resolver B instead. If the readings of the two resolvers do not agree, the operator can initiate bypass of one resolver and use the remaining resolver.

SURVEILLANCE REQUIREMENTS

SR 3.9.4.1

The full-in position indication channels provide input to the one-rod/rod-pair-out interlock and other refueling interlocks which require an all-rods-in permissive. The interlocks are activated when the full-in position indication for any control rod is not present since this indicates that all rods are not fully inserted. Therefore, testing of the full-in position indication channels is performed to ensure that when a control rod is withdrawn, the full-in position indication is not present. Note that failure to indicate full-in when the control rod is not withdrawn results in conservative actuation of the one-rod/rod-pair-out interlock, and therefore, is not explicitly required to be verified by this SR. The full-in position indication channel is considered inoperable even with the control rod fully inserted, if it would continue to indicate full-in with the control rod withdrawn. Performing the SR each time a control rod is withdrawn is considered adequate because of the procedural controls on control rod withdrawals and the visual and audible indications available in the control room to alert the operator of control rods not fully inserted.

BASES

REFERENCES	1.	10 CFR 50, Appendix A, GDC 26.
	2.	Section 15.3.7.

B 3.9 REFUELING OPERATIONS

B 3.9.5 Control Rod OPERABILITY - Refueling

BASES

BACKGROUND	Control rods are components of the Control Rod Drive (CRD) System, the primary reactivity control system for the reactor. In conjunction with the Reactor Protection System (RPS), the CRD System provides the means for the reliable control of reactivity changes during refueling operation. In addition, the control rods provide the capability to maintain the reactor subcritical under all conditions and to limit the potential amount and rate of reactivity increase caused by a malfunction in the CRD System. GDC 26 of 10 CFR 50, Appendix A, requires that one of the two required independent reactivity control systems be capable of holding the reactor core subcritical under cold conditions (Ref. 1). The CRD System is the system capable of maintaining the reactor subcritical in cold conditions. The CRD System also includes the Fine Motion Control Rod Drives (FMCRDs) and the CRD System instrumentation with which the Rod Control and Information System (RC&IS) directly interfaces. The FMCRDs can be inserted either hydraulically or electrically. In response to a scram signal, the FMCRD is inserted hydraulically via the stored energy in the scram accumulators. A redundant signal is also given to insert the FMCRD electrically via its motor drive. This diversity provides a high degree of assurance of rod insertion on demand.
APPLICABLE SAFETY ANALYSES	Prevention and mitigation of prompt reactivity excursions during refueling are provided by refueling interlocks (LCO 3.9.1, "Refueling Equipment Interlocks" and LCO 3.9.2, "Refuel Position One-Rod/Rod-Pair-Out Interlock"), the SDM (LCO 3.1.1, "SHUTDOWN MARGIN (SDM)"), the startup range neutron monitor (SRNM) neutron flux scram (LCO 3.3.1.1, "Reactor Protection System (RPS) Instrumentation" and LCO 3.3.1.2, "Reactor Protection System (RPS) Actuation"), and the control rod block instrumentation (LCO 3.3.2.1, "Control Rod Block Instrumentation").

BASES

APPLICABLE SAFETY ANALYSES (continued)

The safety analysis for the control rod removal error during refueling (Ref. 2) evaluates the consequences of control rod withdrawal during refueling. A prompt reactivity excursion during refueling could potentially result in fuel failure with subsequent release of radioactive material to the environment. Control rod scram provides backup protection should a prompt reactivity excursion occur.

Control Rod OPERABILITY - Refueling satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

Each withdrawn control rod must be OPERABLE. The withdrawn control rod is considered OPERABLE if the scram accumulator pressure is
COL 16.0-1-A 3.9.5-1 ≥ [12.76 MPaG (1850 psig)] and the control rod is capable of being automatically inserted upon receipt of a scram signal. Inserted control rods have already completed their reactivity control function.

APPLICABILITY

During MODE 6, withdrawn control rods must be OPERABLE to ensure that in a scram the control rods will insert and provide the required negative reactivity to maintain the reactor subcritical.

For MODES 1 and 2, control rod requirements are found in LCO 3.1.3, "Control Rod OPERABILITY," LCO 3.1.4, "Control Rod Scram Times," and LCO 3.1.5, "Control Rod Scram Accumulators." During MODES 3, 4, 5, and 6, control rods are not able to be withdrawn since the reactor mode switch is in shutdown and a control rod block is applied. This provides adequate requirements for control rod OPERABILITY during these conditions.

ACTIONS

A.1

With one or more withdrawn control rods inoperable, action must be immediately initiated to fully insert the inoperable control rods. Inserting the control rod ensures that the shutdown and scram capabilities are not adversely affected. Actions must continue until the inoperable control rod is fully inserted.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.9.5.1 and SR 3.9.5.2

During MODE 6, the OPERABILITY of control rods is primarily required to ensure that a withdrawn control rod will automatically insert if a signal requiring a reactor shutdown occurs. Because no explicit safety analysis exists for automatic shutdown during refueling, the shutdown function is satisfied if the withdrawn control rod is capable of automatic insertion and the associated scram accumulator pressure is [≥ 12.76 MPaG (1850 psig)].

COL 16.0-1-A 3.9.5-1

The 7-day Frequency considers equipment reliability, procedural controls over the scram accumulators, and control room alarms and indicating lights, which indicate low accumulator charge pressures.

SR 3.9.5.1 is modified by a Note that allows 7 days after withdrawal of the control rod to perform the Surveillance. This acknowledges that the control rod must first be withdrawn before performance of the Surveillance, and therefore avoids potential conflicts with SR 3.0.1.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 26.
2. Section 15.3.7.

B 3.9 REFUELING OPERATIONS

B 3.9.6 Reactor Pressure Vessel (RPV) Water Level

BASES

BACKGROUND	The movement of fuel assemblies or handling of control rods within the RPV requires a minimum water level of 7.01 m (23.0 ft) above the top of the RPV flange. During refueling, this maintains a sufficient water level above the RPV to retain iodine fission product activity in the water in the event of a fuel handling accident (Ref. 1). Sufficient iodine activity would be retained to limit offsite doses from the accident to < 0.063 Sv (6.3 rem) total effective dose equivalent (TEDE) at the exclusion area boundary and < 0.05 Sv (5.0 rem) TEDE in the control room as required by 10 CFR 52.47(a)(2)(iv) (Ref. 2) and Regulatory Guide 1.183 (Ref. 3) acceptance criteria.
APPLICABLE SAFETY ANALYSES	During movement of irradiated fuel assemblies, which bounds movement of new fuel assemblies and handling of control rods, the water level in the RPV is an initial condition design parameter in the analysis of a fuel handling accident (Ref. 1). A minimum water level of 7.01 m (23.0 ft) allows a decontamination factor of 200 (Ref. 3) 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 cavity water. The fuel pellet to cladding gap is assumed to contain 8% of the total fuel rod iodine inventory (Refs. 1 and 2). A fuel handling accident is assumed to damage all of the fuel rods in two fuel assemblies as discussed in Reference 1. Analysis of the fuel handling accident inside the reactor building is described in Reference 1. With a minimum water level of 7.01 m (23.0 ft) and a minimum decay time of 24 hours prior to fuel handling, the analysis demonstrates that the iodine release due to a postulated fuel handling accident is adequately captured by the water, and that offsite doses are maintained < 0.063 Sv (6.3 rem) TEDE and < 0.05 Sv (5.0 rem) TEDE in the control room as required by 10 CFR 52.47(a)(2)(iv) (Ref. 2) and Regulatory Guide 1.183 (Ref. 3) acceptance criteria.

BASES

APPLICABLE SAFETY ANALYSES (continued)

While the worst case assumptions include the dropping of the irradiated fuel assembly being handled onto the reactor core, the possibility exists of the dropped assembly striking the RPV flange and releasing fission products. Therefore, the minimum depth for water coverage to ensure acceptable radiological consequences is specified from the RPV flange. Since the worst case event results in failed fuel assemblies seated in the core, as well as the dropped assembly, dropping an assembly on the RPV flange will result in reduced releases of fission gases.

RPV Water Level satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

A minimum water level of 7.01 m (23.0 ft) above the top of the RPV flange is required to ensure that the radiological consequences of a postulated fuel handling accident are within acceptable limits, as provided by the guidance of Reference 4.

APPLICABILITY

LCO 3.9.6 is applicable during movement of irradiated fuel assemblies within the RPV and during movement of new fuel assemblies or handling of control rods (i.e., movement with other than the normal control rod drive) within the RPV when irradiated fuel assemblies are seated within the RPV. The LCO minimizes the possibility of a fuel handling accident in the reactor building that is beyond the assumptions of the safety analysis. If irradiated fuel is not being moved and is not present within the RPV, 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 storage pool are covered by LCO 3.7.5, "Fuel Pool Water Level."

ACTIONS

A.1

When the initial conditions for an accident cannot be met, steps should be taken to preclude the accident from occurring. If the water level is < 7.01 m (23.0 ft) above the top of the RPV flange, the movement of fuel assemblies and handling of control rods in the RPV is immediately suspended. Suspension of this activity shall not preclude completion of movement of a component to a safe position. This effectively precludes a fuel handling accident from occurring.

BASES

SURVEILLANCE REQUIREMENTS	SR 3.9.6.1 Verification of a minimum water level of 7.01 m (23.0 ft) above the top of the RPV flange ensures that the design basis for the postulated fuel handling accident analysis during refueling operations is met. Water at the required level limits the consequences of damaged fuel rods, which are postulated to result from a fuel handling accident in the reactor building (Ref. 1). The Frequency of 24 hours is based on engineering judgment and is considered adequate in view of the large volume of water and the normal procedural controls on valve positions, which make significant unplanned level changes unlikely.
REFERENCES	1. Section 15.4.1. 2. 10 CFR 52.47(a)(2)(iv). 3. Regulatory Guide 1.183, July 2000. 4. NUREG-0800, Section 15.7.4.

B 3.9 REFUELING OPERATIONS

B 3.9.7 Decay Time

BASES

BACKGROUND	The movement of irradiated fuel assemblies within the reactor pressure vessel (RPV) requires a minimum decay time of 24 hours to ensure that the initial fission product inventory in the damaged fuel assemblies is less than or equal to the assumptions used in the analysis of a fuel handling accident (Ref. 1). The fission product inventory in the damaged fuel rods in the analysis of a fuel handling accident is based on the days of continuous operation at full power. Due to plant cool down and disassembly operations, there is a time delay following initiation of reactor shutdown before fuel movement operations can be initiated. However, since it may be possible to be ready to move irradiated fuel assemblies in less than 24 hours after subcriticality, requiring a minimum decay time of 24 hours ensures that this assumption is met. Assuming at least 24 hours of decay time, in conjunction with the minimum water level above the top of the RPV flange as required by LCO 3.9.6, "RPV Water Level," and minimum water level above the irradiated fuel assemblies in the spent fuel pools as required by LCO 3.7.5, "Fuel Pool Water Level," is sufficient to limit offsite doses from the accident to < 0.063 Sv (6.3 rem) total effective dose equivalent (TEDE) at the exclusion area boundary and < 0.05 Sv (5.0 rem) TEDE in the control room as required by 10 CFR 52.47(a)(2)(iv) (Ref. 2) and Regulatory Guide 1.183 (Ref. 3) acceptance criteria.
APPLICABLE SAFETY ANALYSES	During movement of irradiated fuel assemblies the fission product inventory in the fuel assemblies is an initial condition design parameter in the analysis of a fuel handling accident (Ref. 1). A decay time of 24 hours ensures the fission product inventory in the fuel rods is less than or equal to the value used in the fuel handling accident analysis. A fuel handling accident is assumed to damage all of the fuel rods in two (2) fuel assemblies as discussed in Reference 1.

BASES

APPLICABLE SAFETY ANALYSES (continued)

Analysis of the fuel handling accident inside the reactor building or fuel building is described in Reference 1. With a minimum water level of 7.01 m (23.0 ft) above the RPV flange and above any irradiated fuel in the spent fuel storage racks, and a minimum decay time of 24 hours prior to fuel handling, the analysis demonstrates that the iodine release due to a postulated fuel handling accident is adequately captured by the water, and that offsite doses are maintained within < 0.063 Sv (6.3 rem) total effective dose equivalent (TEDE) and < 0.05 Sv (5.0 rem) in the control room as required by 10 CFR 52.47(a)(2)(iv) (Ref. 2) and Regulatory Guide 1.183 (Ref. 3) acceptance criteria.

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

LCO

A minimum decay time of 24 hours is required to ensure that the radiological consequences of a postulated fuel handling accident are within acceptable limits, as provided by the guidance of Reference 4.

APPLICABILITY

LCO 3.9.7 is applicable during movement of irradiated fuel assemblies within the RPV. The LCO ensures that the assumptions of the safety analysis of a fuel handling accident in the reactor building or fuel building are met, ensuring that the radiological consequences of a postulated fuel handling accident are within acceptable limits.

ACTIONS

A.1

When the initial conditions for an accident analysis cannot be met, steps should be taken to preclude the accident from occurring. If the reactor has not been subcritical for at least 24 hours, the movement of irradiated fuel assemblies in the RPV is immediately suspended. Suspension of this activity shall not preclude completion of movement of an irradiated fuel assembly to a safe position. This effectively precludes a fuel handling accident from occurring.

BASES

SURVEILLANCE REQUIREMENTS	SR 3.9.7.1 Verification that the reactor has been subcritical for at least 24 hours prior to movement of irradiated fuel in the RPV ensures that the design basis for the postulated fuel handling accident analysis during refueling operations is met. Adequate decay time, and water at the required level, limit the consequences of damaged fuel rods, which are postulated to result from a fuel handling accident in the reactor building or fuel building (Ref. 1).
REFERENCES	1. Section 15.4.1. 2. 10 CFR 52.47(a)(2)(iv). 3. Regulatory Guide 1.183, July 2000. 4. NUREG-0800, Section 15.7.4.

B 3.10 SPECIAL OPERATIONS

B 3.10.1 Inservice Leak and Hydrostatic Testing Operation

BASES

BACKGROUND

The purpose of this Special Operations LCO is to allow certain reactor coolant pressure tests to be performed in MODE 5 when the metallurgical characteristics of the reactor pressure vessel (RPV) require the pressure testing at temperatures > 93.3°C (200°F) (normally corresponding to MODE 3 or 4) or to allow completing these reactor coolant pressure tests when the initial conditions do not require temperatures > 93.3°C (200°F). Furthermore, the purpose is to allow continued performance of control rod scram time testing required by SR 3.1.4.1 or SR 3.1.4.4 if reactor coolant temperatures exceed 93.3°C (200°F) when the control rod scram time testing is initiated in conjunction with an inservice leak or hydrostatic test. These control rod scram time tests would be performed in accordance with LCO 3.10.4, "Control Rod Withdrawal – Cold Shutdown," during MODE 5 operation.

Inservice hydrostatic testing and system leakage pressure tests required by Section XI of the American Society of Mechanical Engineers (ASME) Boiler and Pressure Vessel Code (Ref. 1) are performed prior to the reactor going critical after a refueling outage. The minimum temperatures (at the required pressures) allowed for these tests are determined from the RPV pressure and temperature (P/T) limits required by LCO 3.4.4, "Reactor Coolant System (RCS) Pressure and Temperature (P/T) Limits." These limits are conservatively based on the fracture toughness of the reactor vessel, taking into account anticipated vessel neutron fluence.

With increased reactor vessel fluence over time, the minimum allowable vessel temperature increases at a given pressure. Periodic updates to the RPV P/T limit curves are performed as necessary, based on the results of analyses of irradiated surveillance specimens removed from the vessel. Hydrostatic and leak testing may eventually be required with minimum reactor coolant temperatures > 93.3°C (200°F). However, even with required minimum reactor coolant temperatures < 93.3°C (200°F), maintaining RCS temperatures within a small band during the test can be impractical. Removal of heat addition from reactor core decay heat is coarsely controlled by control rod drive hydraulic system purge flow and reactor water cleanup system non-regenerative heat exchanger

BASES

BACKGROUND (continued)

operation. Test conditions are focused on maintaining a steady state pressure, and tightly limited temperature control poses an unnecessary burden on the operator and may not be achievable in certain instances.

Other testing may be performed in conjunction with the allowances for inservice leak or hydrostatic tests and control rod scram time tests.

APPLICABLE SAFETY ANALYSES

Allowing the reactor to be considered in MODE 5 when the reactor coolant temperature is > 93.3°C (200°F), during, or as a consequence of, hydrostatic or leak testing, or as a consequence of control rod scram time testing initiated in conjunction with an inservice leak or hydrostatic test, effectively provides an exception to MODE 3 and 4 requirements including OPERABILITY of containment and the full complement of redundant Emergency Core Cooling Systems. Since the tests are performed nearly water solid, at low decay heat values, and near MODE 5 conditions, the stored energy in the reactor core will be very low. Under these conditions, the potential for failed fuel and a subsequent increase in coolant activity above the limits of LCO 3.4.3, "RCS Specific Activity," are minimized. In addition, the reactor building refueling and pool area HVAC subsystem (REPAVS) and contaminated area HVAC subsystem (CONAVS) areas will provide a boundary in accordance with this Special Operations LCO to contain airborne radioactivity or steam leaks that could occur during the performance of hydrostatic or leak testing. The required pressure testing conditions provide adequate assurance that the consequences of a steam leak, with the reactor building REPAVS and CONAVS areas isolated, or capable of automatic isolation, will be conservatively bounded by the consequences of the postulated main steam line break (MSLB) outside of containment described in Reference 2. Therefore, requiring the reactor building REPAVS and CONAVS areas to be isolated, or capable of automatic isolation, will conservatively ensure that any potential airborne radiation from steam leaks will be held up, thereby limiting radiation releases to the environment.

In the event of a large primary system leak, the reactor vessel would rapidly depressurize, allowing the low-pressure core cooling systems to operate. The capability of the GDCS subsystems, as required in MODE 5 by LCO 3.5.3, "Gravity-Driven Cooling System (GDCS) – Shutdown," would be more than adequate to keep the core flooded under this low decay heat load condition. Small system leaks would be detected by leakage inspections before significant inventory loss occurred.

BASES

APPLICABLE SAFETY ANALYSES (continued)

For the purposes of this test, the protection provided by normally required MODE 5 applicable LCOs, in addition to the reactor building REPAVS and CONAVS areas requirements of this Special Operations LCO, will ensure acceptable consequences during normal hydrostatic test conditions and during postulated accident conditions.

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

LCO

Operation at reactor coolant temperatures > 93.3°C (200°F) can be in accordance with Table 1.1-1 for MODE 3 or 4 operation without meeting this Special Operations LCO or its ACTIONS. This option may be required due to P/T limits, however, which require testing at temperatures > 93.3°C (200°F). Performance of inservice leak and hydrostatic testing would also necessitate the inoperability of some subsystems normally required to be OPERABLE when > 93.3°C (200°F). Additionally, even with required minimum reactor coolant temperatures < 93.3°C (200°F), RCS temperatures may drift above 93.3°C (200°F) during the performance of inservice leak and hydrostatic testing or during subsequent control rod scram time testing, which is typically performed in conjunction with inservice leak and hydrostatic testing. While this Special Operations LCO is provided for inservice leak and hydrostatic testing, and for scram time testing initiated in conjunction with an inservice leak or hydrostatic test, parallel performance of others tests and inspections is not precluded.

If it is desired to perform these tests while complying with this Special Operations LCO, then the MODE 5 applicable LCOs, in addition to the reactor building REPAVS and CONAVS areas requirements of this Special Operations LCO, must be met. This Special Operations LCO allows changing Table 1.1-1 temperature limits for MODE 5 to "N/A." The additional requirements for reactor building REPAVS and CONAVS areas to be isolated, or capable of automatic isolation, will provide sufficient protection for operations at reactor coolant temperatures > 93.3°C (200°F) for the purposes of performing an inservice leak or hydrostatic test, and for control rod scram time testing initiated in conjunction with an inservice leak or hydrostatic test.

BASES

LCO (continued)	This LCO allows primary containment to be open for frequent, unobstructed access to perform inspections, and for outage activities on various systems to continue consistent with the MODE 5 applicable requirements that are in effect immediately prior to, and immediately after, this operation.
APPLICABILITY	The MODE 5 requirements may only be modified for the performance of, or as a consequence of, the inservice leak or hydrostatic test, or as a consequence of control rod scram time testing initiated in conjunction with an inservice leak or hydrostatic test, so that these operations can be considered as in MODE 5 even though the reactor coolant temperature is > 93.3°C (200°F). The additional requirement for reactor building REPAVS and CONAVS areas to be isolated, or capable of automatic isolation, provides conservatism in the response of the facility to any event that may occur. Operations in all other MODES are unaffected by this LCO.
ACTIONS	A Note has been provided to modify the ACTIONS related to inservice leak and hydrostatic testing operation. Section 1.3, Completion Times, specifies once a Condition has been entered, subsequent divisions, subsystems, components, or variables expressed in the Condition discovered to be inoperable or not within limits, will not result in separate entry into the Condition. Section 1.3 also specifies Required Actions of the Condition continue to apply for each additional failure, with Completion Times based on initial entry into the Condition. However, the Required Actions for each requirement of the LCO not met provide appropriate compensatory measures for separate requirements that are not met. As such, a Note has been provided that allows separate Condition entry for each requirement of the LCO.

BASES

ACTIONS (continued)

A.1 and A.2

Required Actions A.1 and A.2 restore compliance with the normal MODE 5 requirements and thereby exit this Special Operations LCO's Applicability. Activities that could further increase reactor coolant temperature or pressure are suspended immediately in accordance with Required Action A.1 and the reactor coolant temperature is reduced to establish normal MODE 5 requirements. The allowed Completion Time of 24 hours for Required Action A.2 is based on engineering judgment and provides sufficient time to reduce the average reactor coolant temperature from the highest expected value to ≤ 93.3°C (200°F) with normal cooldown procedures.

SURVEILLANCE REQUIREMENTS

SR 3.10.1.1 and SR 3.10.1.2

These Surveillances verify that the appropriate reactor building boundary is available to contain airborne radioactivity or steam leaks that could occur during the performance of hydrostatic or leak testing.

The Surveillances are performed at 24 hour Frequencies to provide appropriate assurance of compliance with these Special Operations LCO requirements.

REFERENCES

1. ASME Boiler and Pressure Vessel Code, Section XI, "Rules for Inservice Inspection of Nuclear Power Plant Components."

2. Subsection 15.4.5.

B 3.10 SPECIAL OPERATIONS

B 3.10.2 Reactor Mode Switch Interlock Testing

BASES

BACKGROUND

The purpose of this Special Operations LCO is to permit operation of the reactor mode switch from one position to another to confirm certain aspects of associated interlocks during periodic tests and calibrations in MODES 3, 4, 5, and 6.

The reactor mode switch is a conveniently located, multi-function, multi-bank, control switch provided to select the necessary scram functions for various plant conditions (Ref. 1). The Reactor Protection System (RPS) selects and bypasses the appropriate trip functions based on the position of the reactor mode switch. For the average power range monitor (APRM), oscillation power range monitor (OPRM), and startup range neutron monitor (SRNM) trip functions the Neutron Monitoring System (NMS) selects and bypasses the functions, not the RPS. The mode switch positions and related scram interlock functions are summarized in Reference 1.

The reactor mode switch also provides interlocks for such functions as control rod blocks, scram accumulator charging water header pressure trip bypass enable, refueling interlocks, and main steam isolation valve isolations.

APPLICABLE SAFETY ANALYSES

The acceptance criterion for reactor mode switch interlock testing is to preclude fuel failure by precluding reactivity excursions or core criticality.

The interlock functions of the shutdown and refuel positions of the reactor mode switch in MODES 3, 4, 5, and 6 are provided to preclude reactivity excursions which could potentially result in fuel failure. Interlock testing which requires moving the reactor mode switch to other positions (run, or startup) while in MODES 3, 4, 5, or 6, requires administratively maintaining all control rods inserted in core cells containing 1 or more fuel assemblies and no CORE ALTERATIONS in progress. There are no credible mechanisms for unacceptable reactivity excursions during the planned interlock testing.

BASES

APPLICABLE SAFETY ANALYSES (continued)

For postulated accidents such as control rod removal error during refueling (Ref. 2) or loading of fuel with a control rod withdrawn, the accident analysis demonstrates that fuel failure will not occur. The withdrawal of a single control rod will not result in criticality when adequate SDM is maintained. Also, loading fuel assemblies into the core with a single control rod withdrawn will not result in criticality thereby preventing fuel failure.

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

LCO

As described in LCO 3.0.7, compliance with this Special Operations LCO is optional. MODE 3, 4, 5, and 6 operations not specified in Table 1.1-1 can be performed in accordance with other Special Operations LCOs (i.e., LCO 3.10.1, "Inservice Leak and Hydrostatic Testing Operation," LCO 3.10.3, "Control Rod Withdrawal - Hot/Stable Shutdown," LCO 3.10.4, "Control Rod Withdrawal - Cold Shutdown," and LCO 3.10.8, "Shutdown Margin (SDM) Test-Refueling") without meeting this LCO or its ACTIONS. If any testing is performed which involves the reactor mode switch interlocks and requires its repositioning beyond that specified in Table 1.1-1 for the current MODE of operation, it can be performed provided all interlock functions potentially defeated are administratively controlled. In MODES 3, 4, 5, and 6 with the reactor mode switch in shutdown per Table 1.1-1, all control rods are fully inserted and a control rod block is initiated. Therefore, all control rods in core cells that contain one or more fuel assemblies must be verified fully inserted while in MODES 3, 4, 5, and 6 with the reactor mode switch in other than the shutdown position.

The additional LCO requirement to preclude CORE ALTERATIONS is appropriate for MODE 6 operations, as discussed below, and is inherently met in MODES 3, 4, and 5 by the definition of CORE ALTERATIONS which cannot be performed with the vessel head in place.

In MODE 6, with the reactor mode switch in the refuel position, only one control rod or control rod pair can be withdrawn under the refuel position one-rod-out interlock (LCO 3.9.2, "Refuel Position One-Rod/Rod-Pair-Out

BASES

LCO (continued)

Interlock"). The refueling equipment interlocks (LCO 3.9.1, "Refueling Equipment Interlocks") appropriately control other CORE ALTERATIONS. Due to the increased potential for error in controlling these multiple interlocks and the limited duration of tests involving the reactor mode switch position, conservative controls are required consistent with MODES 3, 4, and 5 operations. The additional controls of administratively not permitting other CORE ALTERATIONS will adequately ensure that the reactor does not become critical during these tests.

APPLICABILITY

Any required periodic interlock testing involving the reactor mode switch while in MODES 1 and 2 can be performed without the need for Special Operations exceptions. Mode switch manipulations in these MODES would likely result in plant trips. In MODES 3, 4, 5, and 6, this Special Operations LCO is only permitted to be used to allow reactor mode switch interlock testing that cannot conveniently be performed while in other modes. Such interlock testing may consist of required surveillances or calibrations, or may be the result of maintenance, repair, or troubleshooting activities. In MODES 3, 4, 5, and 6, the interlock functions provided by the reactor mode switch in shutdown (i.e., all control rods inserted and incapable of withdrawal) and refueling (i.e., refueling interlocks to prevent inadvertent criticality during CORE ALTERATIONS) positions can be administratively controlled adequately during the performance of certain tests.

ACTIONS

A.1, A.2, A.3.1, and A.3.2

These Required Actions are provided to restore compliance with the Technical Specifications overridden by this Special Operations LCO. Compliance will also result in exiting the Applicability of this Special Operations LCO.

All CORE ALTERATIONS, if in progress, are immediately suspended in accordance with Required Action A.1 and all insertable control rods in core cells that contain one or more fuel assemblies are fully inserted. This will preclude potential mechanisms that could lead to criticality. Suspension of CORE ALTERATIONS shall not preclude the completion of movement of a component to a safe condition. Placing the reactor mode switch to the shutdown position will ensure that all inserted control rods remain inserted and result in operation in accordance with

BASES

ACTIONS (continued)

Table 1.1-1. Alternatively, if in MODE 6, the reactor mode switch must be placed in the refuel position, which will also result in operating in accordance with Table 1.1-1. A Note is added to Required Action A.3.2 to indicate that this Action is not applicable in MODES 3, 4, and 5 since only the shutdown position is allowed in these MODES. The allowed Completion Time of one hour for Required Actions A.2, A.3.1, and A.3.2 provides sufficient time to normally insert the control rods and place the reactor mode switch in the required position based on operating experience and is acceptable given that all operations which could increase core reactivity have been suspended.

SURVEILLANCE REQUIREMENTS

SR 3.10.2.1 and SR 3.10.2.2

Meeting the requirements of this Special Operations LCO maintains operation consistent with or conservative to operating with the reactor mode switch in shutdown (or refuel for MODE 6). The functions of the reactor mode switch interlocks, which are not in effect due to the testing in progress, are adequately compensated for by the Special Operations LCO requirements. The administrative controls to ensure that the operational requirements continue to be met are to be periodically verified. The Surveillances performed at the 12-hour and 24-hour Frequency are intended to provide appropriate assurance that each operating shift is aware of and verify compliance with these Special Operations LCO requirements.

REFERENCES

1. Subsection 7.2.1.5.
2. Subsection 15.3.7.

B 3.10 SPECIAL OPERATIONS

B 3.10.3 Control Rod Withdrawal - Hot / Stable Shutdown

BASES

BACKGROUND	The purpose of this MODES 3 and 4 Special Operations LCO is to permit the withdrawal of a single control rod or control rod pair for testing while in shutdown by imposing certain restrictions. In MODES 3 and 4, the reactor mode switch is in the shutdown position, and all control rods are inserted and blocked from withdrawal. Many systems and functions are not required in these conditions due to other installed interlocks that are actuated when the reactor mode switch is in the shutdown position. However, circumstances will arise while in MODES 3 and 4 which present the need to withdraw a single control rod or control rod pair for various tests (e.g., friction tests, scram timing, and coupling integrity checks). These single control rod or dual control rod withdrawals are normally accomplished by selecting the refuel position for the reactor mode switch. A control rod pair (those associated by a shared control rod drive hydraulic control unit) may be withdrawn by utilizing the SINGLE/GANG rod selection status in the GANG rod selection mode, which "gangs" the two rods together for rod position and control purposes. This Special Operations LCO provides the appropriate additional controls to allow a single control rod, or control rod pair, withdrawal in MODES 3 and 4.
APPLICABLE SAFETY ANALYSES	With the reactor mode switch in the refuel position, the analyses for control rod withdrawal during refueling are applicable and, provided the assumptions of these analyses are satisfied in MODES 3 and 4, these analyses will bound the consequences of an accident. The safety analyses (Ref. 1) demonstrate that the functioning of the refueling interlocks and adequate SHUTDOWN MARGIN (SDM) will preclude unacceptable reactivity excursions. Refueling interlocks restrict the movement of control rods to reinforce operational procedures that prevent the reactor from becoming critical. These interlocks prevent the withdrawal of more than one control rod (or control rod pair). Under these conditions, the core will always be shut down even with the highest worth control rod pair withdrawn if adequate SDM exists.

BASES

APPLICABLE SAFETY ANALYSES (continued)

Control rod pairs have been established for each control rod drive hydraulic control unit (except for the center rod which has its own accumulator). These pairs are selected and analyzed so that adequate SDM is maintained with any control rod pair fully withdrawn.

When the SINGLE/GANG rod selection status in the GANG rod selection mode is used, the selected rod pair is substituted for a single rod within the appropriate logic in order to satisfy the refuel mode one-rod/rod-pair-out interlock. The rod pair may then be withdrawn simultaneously.

The control rod scram function provides backup protection to normal refueling procedures and the refueling interlocks, which prevent inadvertent criticalities during refueling.

Alternate backup protection can be obtained by assuring that a five-by-five array of control rods, centered on each withdrawn control rod, are inserted and incapable of withdrawal.

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

LCO

As described in LCO 3.0.7, compliance with this Special Operations LCO is optional. Operation in MODE 3 and 4 with the reactor mode switch in the refuel position can be performed in accordance with other Special Operations LCOs (i.e., 3.10.2, "Reactor Mode Switch Interlock Testing") without meeting this Special Operations LCO or its ACTIONS. However, if a single control rod or control rod pair withdrawal is desired in MODE 3 or 4, controls consistent with those required during refueling must be implemented and this Special Operations LCO applied. The refueling interlocks of LCO 3.9.2, "Refuel Position One-Rod/Rod-Pair-Out Interlock," required by this Special Operations LCO, will ensure that only one control rod or control rod pair can be withdrawn.

BASES

LCO (continued)

To back up the refueling interlocks (LCO 3.9.2), the ability to scram the withdrawn control rod(s) in the event of an inadvertent criticality is provided by this Special Operations LCO's requirements in Item d.1. Alternately, provided a sufficient number of control rods in the vicinity of the withdrawn control rod(s) are known to be inserted and incapable of withdrawal (Item d.2), the possibility of criticality on withdrawal of these control rods is sufficiently precluded so as not to require the scram capability of the withdrawn control rod(s). Also, once this alternate (Item d.2) is completed, the SDM requirement to account for both the withdrawn-untrippable control rod and the highest worth control rod may be changed to allow the withdrawn-untrippable control rod to be the single highest worth control rod.

APPLICABILITY

Control rod withdrawals are adequately controlled in MODES 1, 2, and 6 by existing LCOs. In MODES 3, 4, and 5, control rod withdrawal is only allowed if performed in accordance with this Special Operations LCO or Special Operations LCO 3.10.4, "Control Rod Withdrawal – Cold Shutdown," and if limited to one control rod or control rod pair. This allowance is only provided with the reactor mode switch in the refuel position. For these conditions, the one-rod/rod-pair-out interlock (LCO 3.9.2), control rod position indication (LCO 3.9.4, "Control Rod Position Indication"), full insertion requirements for all other control rods and scram functions (LCO 3.3.1.1 "Reactor Protection System (RPS) Instrumentation," LCO 3.3.1.2, "Reactor Protection System (RPS) Actuation," LCO 3.3.1.3, "Reactor Protection System (RPS) Manual Actuation," LCO 3.3.1.4, "Neutron Monitoring System (NMS) Instrumentation," LCO 3.3.1.5, "Neutron Monitoring System (NMS) Automatic Actuation") and LCO 3.9.5, "Control Rod OPERABILITY – Refueling," or the added administrative control in Item d.2 of this Special Operations LCO minimizes potential reactivity excursions.

BASES

ACTIONS

A Note has been provided to modify the ACTIONS related to a single control rod or control rod pair withdrawal while in MODES 3 and 4. Section 1.3, Completion Times, specifies once a Condition has been entered, subsequent divisions, subsystems, trains, components or variables expressed in the Condition discovered to be inoperable or not within limits, will not result in separate entry into the Condition. Section 1.3 also specifies Required Actions of the Condition continue to apply for each additional failure, with Completion Times based on initial entry into the Condition. However, the Required Actions for each requirement of the LCO not met provide appropriate compensatory measures for separate requirements that are not met. As such, a Note has been provided that allows separate Condition entry for each requirement of the LCO.

<u>A.1</u>

If one or more of the requirements specified in this Special Operations LCO are not met, the ACTIONS applicable to the stated requirements of the affected LCOs are immediately entered as directed by Required Action A.1. This Required Action has been modified by a Note that clarifies the intent of any other LCO's Required Actions, in accordance with the other applicable LCOs, to insert all control rods and to also require exiting this Special Operations Applicability LCO by returning the reactor mode switch to the shutdown position. A second Note has been added which clarifies that this action is only applicable if the requirements not met are for an affected LCO.

<u>A.2.1 and A.2.2</u>

Required Action A.2.1 and Required Action A.2.2 are alternative ACTIONS that can be taken instead of Required Action A.1 and are provided to restore compliance with the normal MODE 3 or 4 requirements, thereby exiting this Special Operations LCO's Applicability. Actions must be initiated immediately to insert all insertable control rods. Actions must continue until all such control rods are fully inserted. Placing the reactor mode switch in the shutdown position will ensure that all inserted rods remain inserted and restore operation in accordance with Table 1.1-1. The allowed Completion Time of one hour to place the reactor mode switch in the shutdown position provides sufficient time to normally insert the control rods.

BASES

SURVEILLANCE REQUIREMENTS	SR 3.10.3.1, SR 3.10.3.2, and SR 3.10.3.3 The other LCOs made applicable in this Special Operations LCO are required to have their Surveillances met to establish that this Special Operations LCO is being met. If the local array of control rods is inserted and disarmed while the scram function for the withdrawn rod(s) is not available, periodic verification in accordance with SR 3.10.3.2 is required to preclude the possibility of criticality. SR 3.10.3.2 has been modified by a Note that clarifies that this SR is not required to be met if SR 3.10.3.1 is satisfied for LCO 3.10.3.d.1 requirements, since SR 3.10.3.2 demonstrates that the alternative LCO 3.10.3.d.2 requirements are satisfied. Also, SR 3.10.3.3 verifies that all control rods other than the control rod(s) being withdrawn are fully inserted. The 24-hour Frequency is acceptable because of the administrative controls on control rod withdrawals and the protection afforded by the LCOs involved, and hardware interlocks that preclude additional control rod withdrawals.
REFERENCES	1. Subsection 15.3.7.

B 3.10 SPECIAL OPERATIONS

B 3.10.4 Control Rod Withdrawal - Cold Shutdown

BASES

BACKGROUND	The purpose of this MODE 5 Special Operations LCO is to permit the withdrawal of a single control rod or control rod pair for testing or maintenance, while in cold shutdown, by imposing certain restrictions. In MODE 5, the reactor mode switch is in the shutdown position, and all control rods are inserted and blocked from withdrawal. Many systems and functions are not required in these conditions due to the installed interlocks associated with the reactor mode switch in the shutdown position. Circumstances will arise while in MODE 5, however, that present the need to withdraw a single control rod or control rod pair for various tests (e.g., friction tests, scram time testing, and coupling integrity checks). Certain situations may also require the removal of the associated control rod drive(s) (CRDs). These single or dual control rod withdrawals and possible subsequent removals are normally accomplished by selecting the refuel position for the reactor mode switch. A control rod pair (those associated by a single CRD hydraulic control unit) may be withdrawn by utilizing the SINGLE/GANG rod selection status in the GANG rod selection mode, which "gangs" the two rods together for rod position and control purposes. This Special Operations LCO provides the appropriate additional controls to allow a single or dual control rod withdrawal in MODE 5.
APPLICABLE SAFETY ANALYSES	With the reactor mode switch in the refuel position, the analyses for control rod withdrawal during refueling are applicable and, provided the assumptions of these analyses are satisfied in MODE 5, these analyses will bound the consequences of an accident. The safety analyses (Ref. 1) demonstrate that the functioning of the refueling interlocks and adequate SHUTDOWN MARGIN (SDM) will preclude unacceptable reactivity excursions. Refueling interlocks restrict the movement of control rods to reinforce operational procedures that prevent the reactor from becoming critical. These interlocks prevent the withdrawal of more than one control rod or control rod pair. Under these conditions, the core will always be shut down even with the highest worth control rod pair withdrawn if adequate SDM exists.

BASES

APPLICABLE SAFETY ANALYSES (continued)

Control rod pairs have been established for each control rod drive hydraulic control unit (except for the center rod, which has its own accumulator). These pairs are selected and analyzed so that adequate SDM is maintained with any control rod pair fully withdrawn. When the SINGLE/GANG rod selection status is in the GANG rod selection mode, only one rod pair with the same hydraulic control unit can be withdrawn in order to satisfy the refuel mode one-rod/rod-pair-out interlock.

The control rod scram function provides backup protection to normal refueling procedures and the refueling interlocks, which prevent inadvertent criticalities during refueling. Alternate backup protection can be obtained by assuring that a five-by-five array of control rods, centered on the withdrawn control rod(s), are inserted and incapable of withdrawal. This alternate backup protection is required when removing the CRDs because this removal renders the withdrawn control rod(s) incapable of being scrammed.

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

LCO

As described in LCO 3.0.7, compliance with this Special Operations LCO is optional. MODE 5 operations with the reactor mode switch in the refuel position can be performed in accordance with other LCOs (i.e., Special Operations LCO 3.10.2, "Reactor Mode Switch Interlock Testing") without meeting this Special Operations LCO or its ACTIONS. If a single control rod or control rod pair withdrawal is desired in MODE 5, controls consistent with those required during refueling must be implemented and this Special Operations LCO applied. "Withdrawal" in this application includes the actual withdrawal of the control rod(s) as well as maintaining the control rod(s) in a position other than the full-in position, and reinserting the control rod(s).

The refueling interlocks of LCO 3.9.2, "Refuel Position One-Rod/Rod-Pair-Out Interlock," required by this Special Operations LCO will ensure that only one control rod or control rod pair can be withdrawn. At the time CRD removal begins, the disconnection of the position indication probe(s) will cause LCO 3.9.4, "Control Rod Position Indication," and, therefore,

BASES

LCO (continued)

LCO 3.9.2 to fail to be met. Therefore, prior to commencing CRD removal, a control rod withdrawal block is required to be inserted to ensure that no additional control rods can be withdrawn and that compliance with this Special Operations LCO is maintained.
To back up the refueling interlocks (LCO 3.9.2) or the control rod withdrawal block, the ability to scram the withdrawn control rod(s) in the event of an inadvertent criticality is provided by the Special Operations LCO requirements in Item c.1. Alternatively, when the scram function is not OPERABLE, or the CRD is to be removed, a sufficient number of rods in the vicinity of the withdrawn control rod(s) are required to be inserted and made incapable of withdrawal (Item c.2). This precludes the possibility of criticality upon withdrawal of this control rod(s). Also, once this alternate (Item c.2) is completed, the SDM requirement to account for both the withdrawn-untrippable control rod(s) and the highest worth control rod(s) may be changed to allow the withdrawn-untrippable control rod(s) to be the highest worth control rod(s).

APPLICABILITY

Control rod withdrawals are adequately controlled in MODES 1, 2, and 6 by existing LCOs. In MODES 3, 4, and 5, control rod withdrawal is only allowed if performed in accordance with Special Operations LCO 3.10.3, or this Special Operations LCO and if limited to one control rod or control rod pair. This allowance is only provided with the reactor mode switch in the refuel position.

During these conditions, the full insertion requirements for all other control rods, the one-rod/rod-pair-out interlock (LCO 3.9.2), control rod position indication (LCO 3.9.4), and scram functions (LCO 3.3.1.1 "Reactor Protection System (RPS) Instrumentation," LCO 3.3.1.2, "Reactor Protection System (RPS) Actuation," LCO 3.3.1.3, "Reactor Protection System (RPS) Manual Actuation," LCO 3.3.1.4, "Neutron Monitoring System (NMS) Instrumentation," LCO 3.3.1.5, "Neutron Monitoring System (NMS) Automatic Actuation"), and LCO 3.9.5, "Control Rod OPERABILITY – Refueling"), or the added administrative controls in Item b.2 and Item c.2 of this Special Operations LCO, provide mitigation of potential reactivity excursions.

BASES

ACTIONS

A Note has been provided to modify the ACTIONS related to a single control rod or control rod pair withdrawal while in MODE 5. Section 1.3, Completion Times, specifies once a Condition has been entered, subsequent divisions, subsystems, trains, components or variables expressed in the Condition discovered to be inoperable or not within limits, will not result in separate entry into the Condition. Section 1.3 also specifies Required Actions of the Condition continue to apply for each additional failure, with Completion Times based on initial entry into the Condition. However, the Required Actions for each requirement of the LCO not met provide appropriate compensatory measures for separate requirements that are not met. As such, a Note has been provided that allows separate Condition entry for each requirement of the LCO.

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

If one or more of the requirements of this Special Operations LCO are not met with the affected control rod insertable, these Required Actions restore operation consistent with normal MODE 5 conditions (i.e., all rods inserted) or with the exceptions allowed in this Special Operations LCO. Required Action A.1 is modified by two Notes. Note 1 clarifies the intent of any other LCO's Required Actions, in accordance with the other applicable LCOs, to insert all control rods and to also require exiting this Special Operations Applicability LCO by returning the reactor mode switch to the shutdown position. Note 2 has been added to Required Action A.1 to clarify that this action is only applicable if the requirements not met are for an affected LCO.

Required Actions A.2.1 and A.2.2 are specified based on the condition of the control rod(s) being withdrawn. If a control rod is still insertable, actions must be immediately initiated to fully insert all insertable control rods and within one hour, place the reactor mode switch in the shutdown position. Actions must continue until all such control rods are fully inserted. The allowed Completion Time of one hour for placing the reactor mode switch in the shutdown position provides sufficient time to normally insert the control rods.

BASES

ACTIONS (continued)

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

If one or more of the requirements of this Special Operations LCO are not met with the affected control rod(s) not insertable, withdrawal of the control rod and removal of the associated control rod drive must immediately be suspended. If the CRD has been removed such that the control rod is not insertable, these ACTIONS require the most expeditious action be taken to either restore the CRD and insert its control rod or restore compliance with this Special Operations LCO.

SURVEILLANCE REQUIREMENTS

SR 3.10.4.1, SR 3.10.4.2, SR 3.10.4.3, and SR 3.10.4.4

The other LCOs made applicable by this Special Operations LCO are required to have their associated Surveillances met to establish that this Special Operations LCO is being met. If the local array of control rods is inserted and disarmed while the scram function for the withdrawn rod is not available, periodic verification is required to ensure that the possibility of criticality remains precluded. Also, all the control rods are verified to be inserted as well as the control rod withdrawal block. Verification that all the other control rods are fully inserted is required to meet the SDM requirements. Verification that a control rod withdrawal block has been inserted provides assurance that no other control rods can be inadvertently withdrawn under conditions when position indication instrumentation is inoperable for the affected control rod. The 24-hour Frequency is acceptable because of the administrative controls on control rod withdrawals, the protection afforded by the LCOs involved, and hardware interlocks to preclude an additional control rod withdrawal.

SR 3.10.4.2 and SR 3.10.4.4 have been modified by Notes that clarify that these SRs are not required to be met if the alternative requirements demonstrated by SR 3.10.4.1 are satisfied.

REFERENCE

1. Subsection 15.3.7.

B 3.10 SPECIAL OPERATIONS

B 3.10.5 Control Rod Drive (CRD) Removal - Refueling

BASES

BACKGROUND

The purpose of this MODE 6 Special Operations LCO is to permit the removal of a CRD during refueling operations by imposing certain administrative controls. Refueling interlocks restrict the movement of control rods and the operation of the refueling equipment to reinforce operational procedures that prevent the reactor from becoming critical during refueling operations. During refueling operations, no more than one control rod or control rod pair is permitted to be withdrawn from a core cell containing one or more fuel assemblies. The refueling interlocks use the "full in" position indicators to determine the position of all control rods. If the "full in" position signal is not present for every control rod, then the all-rods-in permissive for the refueling equipment interlocks is not present and fuel loading is prevented. Also, the refuel position one-rod/rod-pair-out interlock will not allow the withdrawal of a second control rod. A control rod drive pair (those associated by a shared CRD hydraulic control unit) may be removed under the control of the one-rod/rod-pair-out interlock by utilizing the SINGLE/GANG rod selection status in the GANG rod selection mode. This switch allows the CRD pair to be treated as one CRD for purposes of the one-rod-out interlock.

The control rod scram function provides backup protection to normal refueling procedures, as do the refueling interlocks described above, which prevent inadvertent criticalities during refueling. The requirement for this function to be OPERABLE precludes the possibility of removing the CRD once a control rod is withdrawn from a core cell containing one or more fuel assemblies. This Special Operations LCO provides controls sufficient to ensure that the possibility of an inadvertent criticality is precluded while allowing a single CRD or control rod drive pair to be removed from core cells containing one or more fuel assemblies. The removal of the CRD involves disconnecting the position indication probe, which causes noncompliance with LCO 3.9.4, "Control Rod Position Indication," and, therefore, LCO 3.9.1, "Refueling Equipment Interlocks," and LCO 3.9.2, "Refueling Position One-Rod/Rod-Pair-Out Interlock." The CRD removal also requires isolation of the CRD from the CRD Hydraulic system, thereby causing inoperability of the control rod (LCO 3.9.5, Control Rod OPERABILITY - Refueling).

BASES

APPLICABLE SAFETY ANALYSES

With the reactor mode switch in the refuel position, the analyses for control rod withdrawal during refueling are applicable and, provided the assumptions of these analyses are satisfied, these analyses will bound the consequences of accidents. The safety analyses (Ref. 1) demonstrate that the functioning of the refueling interlocks and adequate SHUTDOWN MARGIN (SDM) will preclude unacceptable reactivity excursions.

Control rod pairs have been established for each control rod drive hydraulic control unit (except for the center rod, which has its own accumulator). These pairs are selected and analyzed so that adequate SDM is maintained with any control rod pair fully withdrawn. When the SINGLE/GANG rod selection status in the GANG rod selection mode is used, the selected rod pair is substituted for a single rod within the appropriate logic in order to satisfy the refuel mode one-rod/rod-pair-out interlock. The rod pair may then be withdrawn simultaneously.

Refueling interlocks restrict the movement of control rods and the operation of the refueling equipment to reinforce operational procedures that prevent the reactor from becoming critical. These interlocks prevent the withdrawal of more than one control rod or control rod pair. Under these conditions, the core will always be shut down even with the highest worth control rod or control rod pair withdrawn if adequate SDM exists. By requiring all other control rods to be inserted and a control rod withdrawal block initiated, the function of the inoperable one-rod/rod-pair-out interlock (LCO 3.9.2) is adequately maintained. This Special Operations LCO requirement to suspend all CORE ALTERATIONS adequately compensates for the inoperable all-rods-in permissive for the refueling equipment interlocks (LCO 3.9.1).

The control rod scram function provides backup protection to normal refueling procedures and the refueling interlocks that prevent inadvertent criticalities during refueling. Since the scram function and refueling interlocks may be suspended, alternate backup protection required by this Special Operations LCO is obtained by assuring that a five-by-five array of control rods, centered on the withdrawn control rod, are inserted and are incapable of being withdrawn (by insertion of a control rod block).

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

BASES

LCO

As described in LCO 3.0.7, compliance with this Special Operations LCO is optional. Operation in MODE 6 with any of the following LCOs – LCO 3.3.1.1, "Reactor Protection System (RPS) Instrumentation," LCO 3.3.1.2 "Reactor Protection System (RPS) Actuation," LCO 3.3.1.3, "Reactor Protection System (RPS) Manual Actuation," LCO 3.3.1.4, "Neutron Monitoring System (NMS) Instrumentation," LCO 3.3.1.5, "Neutron Monitoring System (NMS) Automatic Actuation," LCO 3.9.1, LCO 3.9.2, LCO 3.9.4, or LCO 3.9.5 - not met can be performed in accordance with the Required Actions of these LCOs without meeting this Special Operations LCO or its ACTIONS. However, if a single CRD or CRD drive pair removal from a core cell containing one or more fuel assemblies is desired in MODE 6, controls consistent with those required by LCO 3.3.1.1, LCO 3.3.1.2, LCO 3.3.1.3, LCO 3.3.1.4, LCO 3.3.1.5, LCO 3.9.1, LCO 3.9.2, LCO 3.9.4, and LCO 3.9.5 must be implemented and this Special Operations LCO applied.

By requiring all other control rods to be inserted and a control rod withdrawal block initiated, the function of the inoperable one-rod/rod-pair-out interlock (LCO 3.9.2) is adequately maintained. This Special Operations LCO requirement to suspend all CORE ALTERATIONS (item d) adequately compensates for the inoperable all-rods-in permissive for the refueling equipment interlocks (LCO 3.9.1). Ensuring that the five-by-five array of control rods, centered on each withdrawn control rod, are inserted and incapable of withdrawal adequately satisfies the backup protection that LCO 3.3.1.1, LCO 3.3.1.2, LCO 3.3.1.3, LCO 3.3.1.4, LCO 3.3.1.5, and LCO 3.9.2 would have otherwise provided. Also, once these requirements (Items a, b, and c) are completed, the SDM requirement to account for both the withdrawn-untrippable control rod(s) and the highest worth control rod(s) may be changed to allow the withdrawn-untrippable control rod(s) to be the highest worth control rod(s).

The exception granted in this Special Operations LCO to assume that the withdrawn control rod or control rod pair be the highest worth control rod(s) to satisfy LCO 3.1.1, "SHUTDOWN MARGIN (SDM)," and the inability to withdraw another control rod during this operation without additional SDM demonstrations, is conservative (i.e., the withdrawn control rod or control rod pair may not be the highest worth control rod(s)).

BASES

APPLICABILITY

MODE 6 operations are controlled by existing LCOs. The allowance to comply with this Special Operations LCO in lieu of the ACTIONS of LCO 3.3.1.1, LCO 3.3.1.2, LCO 3.3.1.3, LCO 3.3.1.4, LCO 3.3.1.5, LCO 3.9.1, LCO 3.9.2, LCO 3.9.4, and LCO 3.9.5 is appropriately controlled with the additional administrative controls required by this Special Operations LCO, which reduces the potential for reactivity excursions.

ACTIONS

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

If one or more of the requirements of this Special Operations LCO are not met, the immediate implementation of these Required Actions restores operation consistent with the normal requirements for failure to meet LCO 3.3.1.1, LCO 3.3.1.2, LCO 3.3.1.3, LCO 3.3.1.4, LCO 3.3.1.5, LCO 3.9.1, LCO 3.9.2, LCO 3.9.4, and LCO 3.9.5 (i.e., all control rods inserted) or with the allowances of this Special Operations LCO. The Completion Times for Required Action A.1, Required Action A.2.1, and Required Action A.2.2 are intended to require these ACTIONS be implemented in a very short time and carried through in an expeditious manner to either initiate action to restore the CRD(s) and insert its control rod(s) or restore compliance with this Special Operations LCO. Actions must continue until either required Action A.2.1 or required Action A.2.2 is satisfied.

SURVEILLANCE REQUIREMENTS

SR 3.10.5.1, SR 3.10.5.2, SR 3.10.5.3, SR 3.10.5.4, and SR 3.10.5.5

Verification that all the control rods other than the control rod withdrawn for the removal of the associated CRD are fully inserted is required to assure the SDM is within limits. Verification that the local five-by-five array of control rods other than the control rod withdrawn for the removal of the associated CRD is inserted and disarmed while the scram function for the withdrawn rod is not available is required to ensure that the possibility of criticality remains precluded. Verification that a control rod withdrawal block has been inserted provides assurance that no other control rods can be inadvertently withdrawn under conditions when position indication instrumentation is inoperable for the withdrawn control rod. The Surveillance for LCO 3.1.1, which is made applicable by this Special Operations LCO, is required in order to establish that this Special Operations LCO is being met. Verification that no other CORE ALTERATIONS are being made is required to assure the assumptions of the safety analysis are satisfied.

BASES

SURVEILLANCE REQUIREMENTS (continued)

Periodic verification of the administrative controls established by this Special Operations LCO is prudent to preclude the possibility of an inadvertent criticality. The 24-hour Frequency is acceptable given the administrative controls on control rod removal and hardware interlocks to block an additional control rod withdrawal.

REFERENCES

1. Subsection 15.3.7.

B 3.10 SPECIAL OPERATIONS

B 3.10.6 Multiple Control Rod Withdrawal - Refueling

BASES

BACKGROUND	The purpose of this MODE 6 Special Operations LCO is to permit multiple control rod withdrawal during refueling by imposing certain administrative controls. Refueling interlocks restrict the movement of control rods and the operation of the refueling equipment to reinforce operational procedures that prevent the reactor from becoming critical during refueling operations. During refueling operations, no more than one control rod or control rod pair is permitted to be withdrawn from a core cell containing one or more fuel assemblies. When all four fuel assemblies are removed from a cell the control rods may be withdrawn with no restrictions. Any number of control rods may be withdrawn and removed from the reactor vessel if their cells contain no fuel. The refueling interlocks use the "full in" position indicators to determine the position of all control rods. If the "full in" position signal is not present for every control rod, then the all-rods-in permissive for the refueling equipment interlocks is not present and fuel loading is prevented. Also, the refuel position one-rod/rod-pair-out interlock will not allow the withdrawal of additional control rods. To allow more than one control rod (pair) to be withdrawn during refueling, these interlocks must be defeated. This Special Operations LCO establishes the necessary administrative controls to allow bypass of the "full in" position indicators.
APPLICABLE SAFETY ANALYSES	The safety analyses (Ref. 1) demonstrate that the functioning of the refueling interlocks and adequate SHUTDOWN MARGIN will prevent unacceptable reactivity excursions during refueling. To allow multiple (e.g., more than one control rod or control rod pair) control rod withdrawals, control rod removals, associated control rod drive (CRD) removal, or any combination of these, the "full in" position indication is allowed to be bypassed for each withdrawn control rod if all fuel has been removed from the cell. With no fuel assemblies in the core cell, the associated control rod has no reactivity control function and is not required to remain inserted. Prior to reloading fuel into the cell, however, the associated control rod must be inserted to ensure that an inadvertent criticality does not occur, as evaluated in the Reference 1 analysis.

BASES

APPLICABLE SAFETY ANALYSES (continued)

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

LCO

As described in LCO 3.0.7, compliance with this Special Operations LCO is optional. Operation in MODE 6 with LCO 3.9.3, "Control Rod Position," LCO 3.9.4, "Control Rod Position Indication," or LCO 3.9.5, "Control Rod OPERABILITY – Refueling," not met can be performed in accordance with the Required Actions of these LCOs without meeting this Special Operations LCO or its ACTIONS. If multiple control rod withdrawal or removal or CRD removal is desired, all four fuel assemblies are required to be removed from the associated cells. Prior to entering this LCO any fuel remaining in a cell whose control rod was previously removed under the provisions of another LCO must be removed. "Withdrawal" in this application includes the actual withdrawal of the control rod as well as maintaining the control rod in a position other than the full-in position, and reinserting the control rod.

When loading fuel into the core with multiple control rods withdrawn, special spiral reload sequences are used to ensure that reactivity additions are minimized. Spiral reloading encompasses reloading a cell (four fuel locations immediately adjacent to a control rod) on the edge of a continuous fueled region (the cell can be loaded in any sequence). Otherwise, all control rods must be fully inserted before loading fuel.

APPLICABILITY

Operation in MODE 6 is controlled by existing LCOs. The exceptions from other LCO requirements (e.g., the ACTIONS of LCO 3.9.3, LCO 3.9.4 or LCO 3.9.5) allowed by this Special Operations LCO are appropriately controlled by requiring all fuel to be removed from cells whose "full in" indicators are allowed to be bypassed.

BASES

ACTIONS

A.1, A.2, A.3.1, and A.3.2

If one or more of the requirements of this Special Operations LCO are not met, the immediate implementation of these Required Actions restores operation consistent with the normal requirements for refueling (i.e., all control rods inserted in core cells containing one or more fuel assemblies) or with the exceptions granted by this Special Operations LCO. The Completion Times for Required Action A.1, Required Action A.2, Required Action A.3.1, and Required Action A.3.2 are intended to require that these ACTIONS be implemented in a very short time and carried through in an expeditious manner to either initiate action to restore the affected CRDs and insert their control rods or initiate action to restore compliance with this Special Operations LCO.

SURVEILLANCE REQUIREMENTS

SR 3.10.6.1, SR 3.10.6.2, and SR 3.10.6.3

Periodic verification of the administrative controls established by this Special Operations LCO is prudent to preclude the possibility of an inadvertent criticality. The 24-hour Frequency is acceptable given the administrative controls on fuel assembly and control rod removal, and takes into account other indications of control rod status available in the control room.

REFERENCES

1. Subsection 15.3.7.

B 3.10 SPECIAL OPERATIONS

B 3.10.7 Control Rod Testing - Operating

BASES

BACKGROUND	The purpose of this Special Operations LCO is to permit control rod testing while in MODES 1 and 2 by imposing certain administrative controls. Control rod patterns during startup conditions are controlled by the operator and the rod worth minimizer (RWM) (LCO 3.3.2.1, "Control Rod Block Instrumentation") such that only the specified control rod sequences and relative positions required by LCO 3.1.6, "Rod Pattern Control," are allowed over the operating range from all control rods inserted to the low power setpoint (LPSP) of the RWM. The sequences effectively limit the potential amount and rate of reactivity increase that could occur during a Rod Withdrawal Error (RWE). During these conditions, control rod testing is sometimes required that may result in control rod patterns not in compliance with the prescribed sequences of LCO 3.1.6. These tests may include SDM demonstrations, control rod scram time testing, control rod friction testing, and testing performed during the Startup Test Program. This Special Operations LCO provides the necessary exceptions to the requirements of LCO 3.1.6 and provides additional administrative controls to allow the deviations in such tests from the prescribed sequences in LCO 3.1.6.
APPLICABLE SAFETY ANALYSES	The analytical methods and assumptions used in evaluating the RWE are summarized in Reference 1. RWE analyses assume the reactor operator follows prescribed withdrawal sequences. These sequences define the potential initial conditions for the RWE analyses. The RWM provides backup to operator control of the withdrawal sequences to ensure that the initial conditions of the RWE analyses are not violated. For special sequences developed for control rod testing, the initial control rod patterns assumed in the safety analyses of Reference 1 may not be preserved and, therefore, special RWE analyses are required to demonstrate that these special sequences will not result in unacceptable consequences should a RWE occur during the testing. These analyses are dependent on the specific test being performed.

BASES

APPLICABLE SAFETY ANALYSES (continued)

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

LCO

As described in LCO 3.0.7, compliance with this Special Operations LCO is optional. Control rod testing may be performed, in compliance with the prescribed sequences of LCO 3.1.6, and during these tests no exceptions to the requirements of LCO 3.1.6 are necessary. For testing performed with a sequence not in compliance with LCO 3.1.6, the requirements of LCO 3.1.6 may be suspended provided additional administrative controls are placed on the test to ensure that the assumptions of the special safety analysis for the test sequence remain valid. When deviating from the prescribed sequences of LCO 3.1.6, individual control rods must be bypassed in the Rod Control and Instrumentation System (RC&IS). Assurance that the test sequence is followed can be provided by a second licensed operator or other qualified member of the technical staff verifying conformance to the approved test sequence. These controls are consistent with those normally applied to operation in the startup range as defined in SR 3.3.2.1.9 when it is necessary to deviate from the prescribed sequence (e.g., an inoperable control rod that must be fully inserted).

APPLICABILITY

Control rod testing while in MODES 1 and 2 with THERMAL POWER greater than 10% RTP of the RWM is adequately controlled by the existing LCOs on power distribution limits and control rod block instrumentation. Control rod movement during these conditions is not restricted to prescribed sequences and can be performed within the constraints of LCO 3.2.1, "LINEAR HEAT GENERATION RATE (LHGR)," LCO 3.2.2, "MINIMUM CRITICAL POWER RATIO (MCPR)," and LCO 3.3.2.1. With THERMAL POWER less than or equal to 10% RTP, the provisions of this Special Operations LCO are necessary to perform special tests which are not in conformance with the prescribed control rod sequences of LCO 3.1.6.

BASES

APPLICABILITY (continued)

While in MODES 3 and 4, control rod withdrawal is only allowed if performed in accordance with Special Operations LCO 3.10.3, "Control Rod Withdrawal - Shutdown" or Special Operations LCO 3.10.4, "Control Rod Withdrawal - Cold Shutdown," which provide adequate controls to ensure that the assumptions of the safety analyses of Reference 2 is satisfied. During these Special Operations and while in MODE 6, the one-rod/rod-pair-out interlock (LCO 3.9.2, "Refuel Position One-Rod/Rod-Pair-Out Interlock") and scram functions (LCO 3.3.1.1, "Reactor Protection System (RPS) Instrumentation," LCO 3.3.1.2 "Reactor Protection System (RPS) Actuation," LCO 3.3.1.3, "Reactor Protection System (RPS) Manual Actuation," LCO 3.3.1.4, "Neutron Monitoring System (NMS) Instrumentation," LCO 3.3.1.5, "Neutron Monitoring System (NMS) Automatic Actuation," and LCO 3.9.5, "Control Rod OPERABILITY – Refueling"), or the added administrative controls prescribed in the applicable Special Operations LCOs, minimize potential reactivity excursions.

ACTIONS

A.1

With the requirements of this Special Operations LCO not met (e.g., the control rod pattern not in compliance with the special test sequence), the testing is required to be immediately suspended. Upon suspension of the special test, the provisions of LCO 3.1.6 are no longer exempted and appropriate actions are to be taken either to restore the control rod sequence to the prescribed sequence of LCO 3.1.6 or to shut down the reactor if required by LCO 3.1.6.

SURVEILLANCE REQUIREMENTS

SR 3.10.7.1

During performance of the special test, a second licensed operator or other qualified member of the technical staff is required to verify conformance with the approved sequence for the test. This verification must be performed during control rod movement to prevent deviations from the specified sequence. This Surveillance provides adequate assurance that the specified test sequence is being followed and is also supplemented by SR 3.3.2.1.9, which requires verification of the bypassing of control rods in RC&IS and subsequent movement of these control rods.

BASES

REFERENCES	1.	Section 15.3.8.
	2.	Section 15.3.7.

B 3.10 SPECIAL OPERATIONS

B 3.10.8 SHUTDOWN MARGIN (SDM) Test - Refueling

BASES

BACKGROUND

The purpose of this MODE 6 Special Operations LCO is to permit SDM testing to be performed for those plant configurations in which the reactor pressure vessel (RPV) head is either not in place or the head bolts are not fully tensioned.

LCO 3.1.1, "SHUTDOWN MARGIN (SDM)," requires that adequate SDM be demonstrated following fuel movements or control rod replacement within the RPV. The demonstration must be performed prior to or within 4 hours after criticality is reached. This SDM test may be performed prior to or during the first startup following refueling. Performing the SDM test prior to startup requires the test to be performed while in MODE 6 with the vessel head bolts less than fully tensioned (and possibly with the vessel head removed). While in MODE 6, the reactor mode switch is required to be in the shutdown or refuel position where the applicable control rod blocks ensure that the reactor will not become critical. The SDM test requires the reactor mode switch to be in the startup position since more than one control rod will be withdrawn for the purpose of demonstrating adequate SDM. This Special Operations LCO provides the appropriate additional controls to allow withdrawing more than one control rod from a core cell containing one or more fuel assemblies when the reactor vessel head bolts are less than fully tensioned.

APPLICABLE SAFETY ANALYSES

Prevention and mitigation of unacceptable reactivity excursions during control rod withdrawal, with the reactor mode switch in the startup position while in MODE 6, is provided by the Startup Range Neutron Monitor (SRNM) neutron flux scram and control rod block instrumentation. The limiting reactivity excursion during startup conditions while in MODE 6 is the Rod Withdrawal Error (RWE) event.

RWE analyses assume that the reactor operator follows prescribed withdrawal sequences. For SDM tests performed within these defined sequences, the analyses of Reference 1 are applicable. However, for some sequences developed for the SDM testing, the control rod patterns assumed in the safety analysis may not be met and, therefore, special RWE analyses are required to demonstrate that the SDM test sequence will not result in unacceptable consequences should a RWE occur during the testing. For the purpose of this test, protection provided by the normally required MODE 6 applicable LCOs, in addition

BASES

APPLICABLE SAFETY ANALYSES (continued)

to the requirements of this LCO, will maintain normal test operations as well as postulated accidents within the bounds of the appropriate safety analyses (Ref. 1). In addition to the added requirements for the RWM, APRM, and control rod coupling, the notch movement mode is specified for out-of-sequence withdrawals. Requiring the notch movement mode limits withdrawal steps to a single notch, which limits inserted reactivity and allows adequate monitoring of changes in neutron flux that may occur during the test.

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

LCO

As described in LCO 3.0.7, compliance with this Special Operations LCO is optional. SDM tests may be performed while in MODE 2 in accordance with Table 1.1-1 without meeting this Special Operations LCO or its ACTIONS. For SDM tests performed while in MODE 6, additional requirements must be met to ensure that adequate protection against potential reactivity excursions is available. To provide additional scram protection, beyond the normally required SRNMs, the APRMs are also required to be OPERABLE (LCO 3.3.1.1, "Reactor Protection System (RPS) Instrumentation," Function 2, LCO 3.3.1.2, "Reactor Protection System (RPS) Actuation," LCO 3.3.1.4 "Neutron Monitoring System (NMS) Instrumentation," Functions 2.a and 2.d, and LCO 3.3.1.5, "Neutron Monitoring System (NMS) Automatic Actuation," Function 2) as though the reactor were in MODE 2. Because multiple control rods will be withdrawn and the reactor will potentially become critical, the approved control rod withdrawal sequence must be enforced by the RWM (LCO 3.3.2.1, "Control Rod Block Instrumentation", Function 1.b, MODE 2), or must be verified by a second licensed operator or other qualified member of the technical staff. To provide additional protection against an inadvertent criticality, control rod withdrawals that do not conform to the ganged withdrawal sequence restrictions (GWSR) specified in LCO 3.1.6, "Rod Pattern Control" (i.e., out-of-sequence control rod withdrawals) must be made in the notch movement mode to minimize the potential reactivity insertion associated with each movement. Coupling integrity of withdrawn control rods is required to minimize the probability of a RWE and ensure proper functioning of the withdrawn control rods if required to scram. Because the reactor vessel

BASES

LCO (continued)

head may be removed during these tests, no other CORE ALTERATIONS may be in progress. In addition, the reactor building refueling and pool area HVAC subsystem (REPAVS) and contaminated area HVAC subsystem (CONAVS) areas will provide a boundary as required to mitigate the consequences of an inadvertent criticality. This Special Operations LCO then allows changing the Table 1.1-1 reactor mode switch position requirements to include the startup position such that the SDM tests may be performed while in MODE 6.

APPLICABILITY

These SDM test Special Operations requirements are only applicable if the SDM tests are to be performed while in MODE 6 with the reactor vessel head removed or the head bolts not fully tensioned. Additional requirements during these tests to enforce control rod withdrawal sequences and restrict other CORE ALTERATIONS provide protection against potential reactivity excursions. Operations in all other MODES are unaffected by this LCO.

ACTIONS

A.1 and A.2

With one or more control rods discovered uncoupled during this Special Operation, a controlled insertion of each uncoupled control rod is required. Operation may continue, provided the control rods are fully inserted within 3 hours and disarmed within 4 hours. Inserting a control rod ensures the shutdown and scram capabilities are not adversely affected. The control rod is disarmed to prevent inadvertent withdrawal during subsequent operations. Required Action A.1 is modified by a Note that allows control rods to be bypassed in accordance with SR 3.3.2.1.9, if required, to allow insertion of inoperable control rod and continued operation. SR 3.3.2.1.9 provides additional requirements when the control rods are bypassed to ensure compliance with the RWE analysis.

The allowed Completion Times are reasonable, considering the small number of allowed inoperable control rods, and provide time to insert and disarm the control rods in an orderly manner without challenging plant systems.

BASES

ACTIONS (continued)

Condition A is modified by a Note allowing separate Condition entry for each uncoupled control rod. This is acceptable since the Required Actions for this Condition provide appropriate compensatory actions for each uncoupled control rod. Complying with the Required Actions may allow for continued operation. Subsequent uncoupled control rods are governed by subsequent entry into the Condition and application of the Required Actions.

B.1

With one or more of the requirements of this LCO not met, for reasons other than an uncoupled control rod, the testing should be immediately stopped by placing the reactor mode switch in the shutdown or refuel position. This results in a condition that is consistent with the requirements for MODE 6 where the provisions of this Special Operations LCO are no longer required.

SURVEILLANCE REQUIREMENTS

SR 3.10.8.1, SR 3.10.8.2, and SR 3.10.8.3

LCO 3.3.1.1 Function 2, LCO 3.3.1.2, LCO 3.3.1.4, Functions 2.a and 2.d, and LCO 3.3.1.5, Function 2 made applicable in this Special Operations LCO, are required to have applicable Surveillances met to establish that this Special Operations LCO is being met. However, the control rod withdrawal sequences during the SDM tests may be enforced by the RWM (LCO 3.3.2.1, Function 1.b, MODE 2 requirements) or by a second licensed operator or other qualified member of the technical staff. As noted, either the applicable SRs for the RWM (LCO 3.3.2.1) must be satisfied according to the applicable Frequencies (SR 3.10.8.2), or the proper movement of control rods must be verified (SR 3.10.8.3). This latter verification (i.e., SR 3.10.8.3) must be performed during control rod movement to prevent deviations from the specified sequence. These surveillances provide adequate assurance that the specified test sequence is being followed.

SR 3.10.8.4

Periodic verification of the administrative controls established by this LCO will ensure that the reactor is operated within the bounds of the safety analysis. The 12 hour Frequency is intended to provide appropriate assurance that each operating shift is aware of and verifies compliance with these Special Operations LCO requirements.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.10.8.5 and SR 3.10.8.6

These Surveillances verify that the appropriate reactor building boundary is available to mitigate the consequences of an inadvertent criticality.

The Surveillances are performed at 24 hour Frequencies to provide appropriate assurance of compliance with these Special Operations LCO requirements.

SR 3.10.8.7

Coupling verification is performed to ensure the control rod is connected to the control rod drive mechanism and will perform its intended function when necessary. The verification is required to be performed prior to declaring the control rod OPERABLE after work on the control rod or CRD System that could affect coupling. This Frequency is acceptable considering the low probability that a control rod will become uncoupled when it is not being moved and operating experience related to uncoupling events.

REFERENCES

1. Subsection 15.3.8.

B 3.10 SPECIAL OPERATIONS

B 3.10.9 Oxygen Concentration - Startup Test Program

BASES

BACKGROUND	Testing performed as part of the Startup Test Program (Ref. 1), requires containment entries to inspect components following the performance of some tests. LCO 3.6.1.8, "Containment Oxygen Concentration," requires the containment to be inerted with the oxygen concentration maintained below 4.0 volume percent (v/o). This Special Operations LCO provides appropriate restriction to allow containment entries for the required Startup Test Program without having increased personnel risks due to an oxygen deficient atmosphere.
APPLICABLE SAFETY ANALYSES	The containment oxygen concentration is maintained below 4.0 v/o to ensure that an event which produces any amount of hydrogen does not result in a combustible mixture inside containment. The time allowed with the requirements for containment inerting suspended is sufficiently short such that the probability of an event requiring an inerted atmosphere is very low. Additionally, due to the minimal exposure of the fuel, the decay heat and fission product levels are not significant. As described in LCO 3.0.7, compliance with Special Operations LCOs is optional and therefore no specific criteria of 10 CFR 50.36(c)(2)(ii) applies. Special Operations LCOs provide flexibility to perform certain operations by appropriately modifying requirements of other LCOs.
LCO	As described in LCO 3.0.7, compliance with this Special Operations LCO is optional. However, to perform portions of the Startup Test Program it is impractical to have the containment inerted. To minimize the probability of an accident that assumes an inerted containment, the requirements of LCO 3.6.1.8 are only allowed to be suspended during the initial 120 effective full power days of operation.
APPLICABILITY	Suspension of the requirements for containment inerting with THERMAL POWER > 15% RTP are applied during the Startup Test Program up to 120 effective full power days of operation. This minimizes the probability of an event requiring an inerted containment and also minimizes the decay heat and fission product levels in the fuel.

BASES

ACTIONS	A.1 With the requirements of the LCO not met, the provisions of LCO 3.6.1.8 are no longer exempted and the appropriate ACTIONS of the affected LCO (LCO 3.6.1.8) are required to be taken. The Required Action is provided to restore compliance with the Technical Specification overridden by this Special Operations LCO. Compliance will also result in exiting the Applicability of this Special Operations LCO.
SURVEILLANCE REQUIREMENTS	SR 3.10.9.1 Periodic verification of the allowed 120 effective full power days of operation established by the LCO provides adequate assurance the reactor is operated within the bounds of the LCO. The 7-day Frequency is acceptable given the slow and predictable change in time of core operation.
REFERENCES	1. Chapter 14.

B 3.10 SPECIAL OPERATIONS

B 3.10.10 Oscillation Power Range Monitor (OPRM) - Initial Cycle

BASES

BACKGROUND	The OPRMs provide trip signals to the RPS. The OPRM trip protection includes algorithms that detect thermal hydraulic instability (flux oscillation with unacceptable amplitude and frequency) as described in the Bases for LCO 3.3.1.4, "NMS Instrumentation." To ensure adequate implementation of the OPRM algorithms and to avoid unnecessary spurious reactor scrams, the system will be checked during the startup test program. Final OPRM configuration development and deployment to achieve better balance between defense-in-depth protection and inadvertent scram avoidance would be implemented prior to startup from the first cycle refueling outage. During the initial cycle, reactor instability protection is provided by the backup stability protection (BSP) (Ref. 1). If the entry to the BSP region (as defined in Ref. 1) is inadvertent or forced, immediate exit from the region is required. The region can be exited by control rod insertion or FW temperature maneuvering. The guidance and actions recommended by the BSP emphasize instability prevention to minimize the burden placed on the operator when monitoring for the onset of power oscillations. Therefore, caution is required whenever operating near the BSP Region boundary, and it is recommended that the amount of time spent operating near this region be minimized
APPLICABLE SAFETY ANALYSES	The OPRM – Upscale Function is not credited in the safety analysis and is included in the Technical Specifications as a defense-in-depth feature. The OPRM – Upscale Function is provided as a backup to other RPS Functions and the Selected Control Rod Run-In/ Select Rod Insert (SCRRI/SRI) function. As such, the BSP (Ref. 1) provides adequate protection for the initial cycle of operation. As described in LCO 3.0.7, compliance with Special Operations LCOs is optional and therefore no specific criteria of 10 CFR 50.36(c)(2)(ii) applies. Special Operations LCOs provide flexibility to perform certain operations by appropriately modifying requirements of other LCOs.

BASES

LCO	As described in LCO 3.0.7, compliance with this Special Operations LCO is optional. However, to perform the OPRM checkout and minimize the potential for unnecessary spurious reactor scram, the requirements for OPRM OPERABILITY are allowed to be suspended. Appropriately trained on-shift operations staff can implement the alternate method to detect and suppress thermal hydraulic instability oscillations (Ref. 1) should they occur.
APPLICABILITY	Suspension of the requirements for OPRM OPERABILITY is allowed during the initial cycle of operation. To ensure adequate implementation of the OPRM algorithms and to avoid unnecessary spurious reactor scrams, the system is evaluated during the startup test program. Any necessary OPRM configuration development and deployment is implemented prior to startup from the first cycle refueling outage.
ACTIONS	A.1 With the requirements of the LCO not met, ACTIONS appropriate to inoperable OPRM consistent with the actions of LCO 3.3.1.4 and LCO 3.3.1.5 are required. In this condition, the plant must be brought to a MODE or other specified condition in which the LCO does not apply. To achieve this status, THERMAL POWER must be reduced to < 25% RTP within 4 hours. The 4 hour Completion Time is reasonable, based on engineering judgment, to reduce THERMAL POWER to < 25% RTP in an orderly manner and without challenging plant systems. Compliance will also result in exiting the Applicability of this Special Operations LCO.
SURVEILLANCE REQUIREMENTS	SR 3.10.10.1 Periodic verification of on-shift operations staff training on alternate method to detect and suppress thermal hydraulic instability oscillations supports this Special Operation allowance. The 92-day Frequency is acceptable to provide reasonable assurance of the necessary operations staff training for BSP.
REFERENCES	1. Section 4D.3.3.