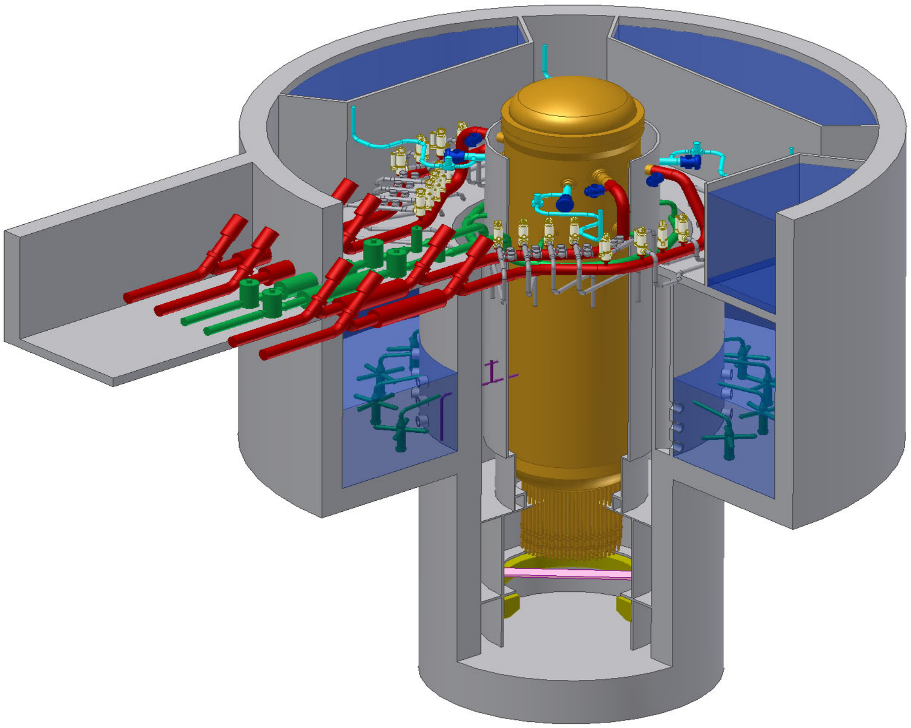
GE Nuclear Energy

26A6642BT
Revision 0
August 2005



ESBWR Design Control Document

Tier 2

Chapter 16B

Bases

(Conditional Release - pending closure of design verifications)

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. A MCPR limit is to be established to preclude violation of the SL that 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 MCPR limit.

2.1.1.1 Fuel Cladding Integrity

GE critical power correlations are applicable for all critical power calculations at pressures ≥ [ ] MPa gauge ([ ] psig) and core flows ≥ [ ]% of rated flow. For operation at low pressures or low flows, another basis is used, as follows:

[ ]

2.1.1.2 MCPR

The fuel cladding integrity SL 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 SL is not violated during normal operations and AOOs, considering the power distribution within the core and all uncertainties.

The probability of the occurrence of boiling transition is determined using the approved General Electric Critical Power correlations. Details of the fuel cladding integrity SL calculation process are given in References [4], [5] and [6]. Reference [7] describes the methodology for determining the transient uncertainties and the process for calculating the operating limit MCPR. The steady state uncertainties used in the statistical analysis are provided in Reference [8].

BASES

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 to a level of [ ]. 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 and to also provide adequate margin for effective action.

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.

SAFETY LIMIT VIOLATIONS

Exceeding a SL may cause fuel damage and create a potential for radioactive releases in excess of 10 CFR 100, "Reactor Site Criteria," limits (Ref. 3). 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. NEDE-24011-P-A, [latest approved revision].]

3. 10 CFR 100.

[4. NEDE-10958-PA, "General Electric BWR Thermal Analysis Basis (GETAB): Data, Correlation and Design Application", January 1977.]

BASES

[5. NEDC-32601-P-A, “Methodology and Uncertainties for Safety Limit MCPR Evaluations”, August 1999.]

[6. NEDC-32694-P-A, “Power Distribution Uncertainties for Safety Limit MCPR Evaluations”, August 1999.]

[7. NEDE-32906-P-A, Rev. 1, “TRACG Application for Anticipated Operational Occurrences (AOO) Transient Analyses”, April 2003.]

[8. The documentation that defines the ESBWR specific uncertainties.]

B 2.0 SAFETY LIMITS (SLs)

B 2.1.2 Reactor Coolant System (RCS) Pressure SL

BASES

BACKGROUND

The SL on reactor steam dome 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 steam dome 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 (ISLH) 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 100, "Reactor Site Criteria" (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, [1974 Edition], including Addenda through the [2003] (Ref. 5), which permits a maximum pressure transient

BASES

	of 110%, [ ] MPa gauge (1375 psig), of design pressure 1250 psig. The SL of [ ] MPa gauge ([ ] psig), as measured in the reactor steam dome, is equivalent to [ ] MPa gauge (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 [ ] MPa gauge (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 [ ] MPa gauge ([ ] psig) as measured at the reactor steam dome.
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 100, "Reactor Site Criteria," limits (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 100.
5. ASME, Boiler and Pressure Vessel Code, [1974 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

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

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 4 and 73 hours to initiate actions to place the unit 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 4, 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 3.7.4, Fuel Pool Water Level. LCO 3.7.4 has an Applicability of “During movement of irradiated fuel assemblies 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 3.7.4 are not met while in MODES 1, 2, 3, or 4, there is no safety benefit to be gained by placing the unit in a shutdown condition. The Required Action of LCO 3.7.4 of “Suspend movement of irradiated fuel assemblies in the associated fuel storage pool(s)” is the appropriate Required Action to complete in lieu of the actions of LCO 3.0.3. These exceptions are addressed in the individual Specifications.

MODES 3 and 4 correspond to passive safety-related system capabilities for long-term decay heat removal. MODES 3 and 4 provide safe shutdown within safety-related system capabilities while maintaining operational conditions consistent with risk and providing greater operational flexibility.

The Commission approved the staff recommendation (from SECY-94-084) that “EPRI’s proposed 215.6°C (420°F) or below, rather than the cold shutdown condition required by RG 1.139, as a safe stable condition, which the" ESBWR's passive decay heat removal systems (Isolation Condensers) are capable of achieving and maintaining following non-LOCA events for at least 72 hours without operator action. Operator action is credited after 72 hours to refill the Isolation Condenser pools or initiate non-safety shutdown cooling.

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, 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, there is a small subset of systems and components that have been determined to be more important to risk and use of the LCO 3.0.4.b allowance is prohibited. The LCOs governing these systems and components contain Notes prohibiting the use of LCO 3.0.4.b by stating that LCO 3.0.4.b is not applicable.

LCO 3.0.4.c allows entry into a MODE or other specified condition in the Applicability with the LCO not met based on a Note in the Specification which states LCO 3.0.4.c is applicable. These specific allowances permit entry into MODES or other specified conditions in the Applicability when the associated ACTIONS to be entered do not provide for continued operation for an unlimited period of time and a risk assessment has not been performed. This allowance may apply to all the ACTIONS or to a

BASES

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.

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, and MODE 3 to MODE 4.

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:

BASES

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

b. The OPERABILITY of other equipment.

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

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 n 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 support systems that have an LCO specified in the Technical Specifications (TS). This exception is provided because LCO 3.0.2 would require that the Conditions and Required Actions of the associated inoperable supported system LCO be entered solely due to the inoperability of the support system. This exception is justified because the actions that are required to ensure the 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 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 is 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.

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 addresses 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 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.

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:

a. Control Rod Drive maintenance during refueling that requires scram testing at > [6.550 MPa gauge (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 [6.550 MPa gauge (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

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.

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 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) 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, and MODE 3 to MODE 4.

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.

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 accidents (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 (Ref. 4). 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. 5).
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

C.1

With SDM not within limits in MODE 3 and 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 within 1 hour to provide means for control of potential radioactive releases. This includes ensuring the Reactor Building is OPERABLE. Actions must continue until the Reactor Building is OPERABLE.

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 within 1 hour to provide means for control of potential radioactive releases. This includes ensuring the Reactor Building is OPERABLE. Actions must continue until the Reactor Building is OPERABLE.

SURVEILLANCE REQUIREMENTS

SR 3.1.1.1

Adequate SDM is verified to ensure the reactor can be made subcritical from any initial operating condition. This can be accomplished by a test, an evaluation, or a combination of the two. 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. 3). 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 as specified in the COLR 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 5, 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 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

BASES

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. [NEDE-24011-P-A, “General Electric Standard Application for Reactor Fuel,” September 1988.

3. Section 15.4.1.

4. Hatch-1 FSAR, Amendment 24, Question 3.6.7, December 1972.

5. Section 4.3.]

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

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. 1). 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 satisfies 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.

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

BASES

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 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

SURVEILLANCE REQUIREMENTS	<u>SR 3.1.2.1</u> 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. 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 stepping 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 [4 and 5].
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

BASES

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 MCPR 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. 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.

BASES

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 5 are located in LCO 3.9.5, "Control Rod OPERABILITY - Refueling."

ACTIONS

The ACTIONS Table is modified by a Note that 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.

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

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. SR 3.3.2.1.6 provides additional requirements when control rods are bypassed in RC&IS to ensure compliance with the RWE analysis. 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, the 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 placing the rod in RC&IS in Bypass or by manually 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 outage time "clock." The Required Action A.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 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 4conditions. In addition, Required Action A.3 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.3 is acceptable.

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 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 disconnecting power to the motor drive or by placing the rod in RC&IS Inop Bypass. Required Action C.1 is modified by a Note that allows control rod to be bypassed in the RC&IS if required to allow insertion of the inoperable control rods and continued operation. SR 3.3.2.1.6 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

At ≤ 10% RTP, the generic GWSR (which is equivalent to previous banked position withdrawal sequence (BPWS) analysis) 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. 6). 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 separated by at least two OPERABLE control rods, 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) 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 at two notches 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 Gang 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.

SR 3.1.3.4

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 LOGIC SYSTEM FUNCTIONAL TEST in LCO 3.3.1.1, "Reactor Protection System (RPS) Instrumentation," 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 blade 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, considering 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

BASES

uncoupling cannot be accomplished unless the associated orificied 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 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 orificied fuel support has been moved.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 26, GDC 27, GDC 28, and GDC 29.
2. [NEDE-24011-P-A, “General Electric Standard Application for Reactor Fuel,” September 1988.
3. Section 4.6.
4. Section 7.7
5. Section 15.4.
6. Section 15.4.
7. NEDO-21231, “Banked Position Withdrawal Sequence,” Section 7.2, January 1977.]

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 two fine motion control rod drives (FMCRDs). When a scram signal is initiated, control air is vented from the scram valve in each 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, and 5]. 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.

The scram function of the CRD System protects the MCPR 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 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. Above [6.550 MPa gauge (950 psig)], the scram function is designed to insert negative reactivity at a rate fast enough to prevent the actual MCPR from becoming less than the MCPR SL during the analyzed limiting power transient. Below [6.550 MPa gauge (950 psig)] the scram function is assumed to function during the rod withdrawal error event (RWE) (Ref. 5) 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 times 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 times specified in Table 3.1.4-1 are faster than those assumed in the design basis analysis. The scram times 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 times are specified as a function of reactor steam dome pressure to account for the pressure dependence of the scram times. The scram times are specified relative to percent insertion. The scram times 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.

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.

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

BASES

considered inoperable as required by SR 3.1.3.4, and are not considered slow .

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

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.

SURVEILLANCE REQUIREMENTS

All four SRs of this LCO are modified by a Note stating that during a single control rod 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 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 ≥ 6.550 MPa gauge (950 psig) demonstrates acceptable scram times for the transients analyzed in References [3 and 4].

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 ≥ [6.550 MPa gauge (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.". If more than 7.5% of the sample is declared to be “slow” per the 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 satisfied, or until the total number of "slow" control rods (throughout the core, from all Surveillances) exceeds the LCO limit. 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 120 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

BASES

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 < [6.550 MPa gauge (950 psig)] are established based on a high probability of meeting the acceptance criteria at reactor pressures ≥ [6.550 MPa gauge (950 psig)]. Limits for reactor pressures ≥ [6.550 MPa gauge (950 psig)] are found in Table 3.1.4-1. If testing demonstrates the affected control rod does not meet these limits, but is within [ ] second limit of Table 3.1.4-1, Note 2, the control rod can be declared OPERABLE and "slow."

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.

<u>SR 3.1.4.4</u>

After fuel movement has occurred within the affected cell or after work on control rod or 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 ≥ 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.

BASES

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. [NEDE-24011-P-A, “General Electric Standard Application for Reactor Fuel”, September 1988].

3. Section 4.6.

4. Section 5.2.

5. [Section 15.4.]

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 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 MCPR 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 satisfies 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 CRD 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 the ability of the accumulator to still be able to scram the associated control rod(s) and 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 [12.755 MPa gauge (1850 psig)] is well below the expected pressure of [14.824 MPa gauge (2150 psig)] (Ref. 2).

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. [NEDE-24011-P-A, “General Electric Standard Application Fuel”, September 1988.
2. [Section 4.6].
3. Section 5.2.
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), 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 References 1 and 2. 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 References 1 and 2 follow the Gang Withdrawal Sequence Restrictions (GWSR), which is the ESBWR equivalent of the BPWS described in Reference 3. 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 (Ref. 4). Since the failure consequences for UO_2 have been shown to be insignificant below fuel energy depositions of 300 cal/gm, the fuel damage limit of 280 cal/gm provides a margin of safety to significant core damage and release of radioactivity (Ref. 4). Generic analysis of the GWSR (BPWS, Ref. 3) has demonstrated that the 280 cal/gm fuel damage limit will not be violated during a postulated reactivity transient while following the GWSR mode of operation. The generic analysis also evaluated the effect of fully inserted inoperable control rods not in compliance with the sequence to allow a

BASES

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).

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, 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 280 cal/gm fuel damage limit during a 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

BASES

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 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 3.3.2.1.6 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. NEDE-24011-P-A-9, “General Electric Standard Application for Reactor Fuel - Supplement for United States”, September 1988.

BASES

2. Section 15.3.

3. NEDO-21231, “Banked Position Withdrawal Sequence,” January 1977.]

4. NUREG-0800, “Standard Review Plan,” Section 15.4.1, Revision 2, July 1981.]

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.7 Standby Liquid Control (SLC) System

BASES

BACKGROUND

The SLC System is designed, to automatically provide the capability of 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 the requirements of 10 CFR 50.62 (Ref. 1) on anticipated transient without scram (ATWS).

The SLC System contains two identical and separate trains. Each SLC train consists of a nitrogen pressurized accumulator tank containing sodium pentaborate solution (SPBS) and is connected by piping through two parallel injection squib valves to the Reactor Pressure Vessel (RPV). The SPBS is injected into the RPV by firing squib valves. Each injection line shall be connected to a 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 position 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. The only power source required for igniting the squib explosives is safety related 250 VDC. Adequate functioning of the SLC System shall be assured if only one of the two injection valves open in each SLC train. The SLC System can be started automatically or manually from the control room. The accumulator tanks can be isolated manually or automatically from a low accumulator level instrumentation.

The SLC System is also credited in the loss of coolant accident (LOCA) to provide makeup water to the RPV. The emergency core cooling system (ECCS) and the SLC are 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 and SLC, in conjunction with the containment, limits the release of radioactive materials to the environment following a LOCA.

APPLICABLE SAFETY

The SLC System is automatically initiated when both the average power range monitor (APRM) is not downscale and either high reactor vessel

BASES

ANALYSES

dome pressure or low reactor vessel water level (Level 2) persists for at least 3 minutes. The SLC System is manually initiated from the main control room as directed by the emergency operating procedures if the operator believes the reactor cannot be shut down, or kept shut down, with the control rods. The SLC System is used in the event that not enough control rods can be inserted to accomplish shutdown and cooldown in the normal manner. 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, it is necessary to inject a quantity of boron which produces a concentration of 760 ppm of natural boron 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. 2). That result is then increased by a factor of 1.15 to provide a further margin of 15% to discount potential dilution by the RWCU/SDC system when activated in the shutdown cooling mode.

In addition, under conditions of a LOCA, the SLC will also be initiated to provide makeup water to the vessel to ensure the core is cooled.

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 tank and the availability of a flow path from each accumulator tank to the RPV, including the OPERABILITY of the instrumentation and valves. For a LOCA, the volume of water in the SLCs tanks are necessary for makeup and core cooling. Two SLC trains are required to be OPERABLE, each containing two OPERABLE injection squib valves and associated piping, valves, and instruments and controls to ensure an OPERABLE flow path.

APPLICABILITY

In MODES 1 and 2, the SLC System is needed for both its shutdown capability and for RPV water makeup and core cooling. In MODES 3 and 4, the SLC is also needed for RPV water makeup and core cooling

---

capability. In MODE 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 controls to ensure the reactor remains subcritical. In MODE 5, only a single control rod can be withdrawn from a core cell containing fuel assemblies. Demonstration of adequate SDM (LCO 3.1.1, "SHUTDOWN MARGIN (SDM)") ensures that the reactor will not become critical. Therefore, the SLC System is not required to be OPERABLE during these conditions when only a single control rod can be withdrawn.

ACTIONS

A.1

If the concentration of sodium pentaborate in solution in one or more acccumulator tanks 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 3. These additional features provide the sufficient 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.

B.1

With one injection squib valve flow path in one or two 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 path are adequate to perform the shutdown function. However, the overall reliability is reduced because a single failure in the remaining OPERABLE squib valve flow path could result in reduced SLC System capability. The 7 day Completion Time is based on the availability of an OPERABLE train capable of performing the intended SLC System function and the low probability of a Design Basis Accident (DBA) or transient occurring concurrent with the failure of the Control Rod Drive System to shut down the plant.

C.1

If the SLC System is inoperable for reasons other than Condition A or B, at least one train must be restored to OPERABLE status within 8 hours. The allowed Completion Time of 8 hours is considered acceptable, given

BASES

the low probability of a DBA or transient occurring concurrent with the failure of the control rods to shut down the reactor.

D.1

If any 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 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 3.1.7.1, 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 tank, temperature of the room containing the boron accumulators, piping, and valves, and nitrogen pressure in each accumulator tank), thereby ensuring the SLC System OPERABILITY without disturbing normal plant operation. These Surveillances ensure the proper SPBS volume and temperature and accumulator nitrogen pressure are maintained. Maintaining a minimum specified SPBS temperature is important in ensuring that the boron remains in solution and does not precipitate out in the accumulator tanks or in the injection piping. Maintaining a minimum accumulator 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 in the measured parameters of volume and temperature.

SR 3.1.7.4 and SR 3.1.7.5

SR 3.1.7.4 verifies the continuity of the explosive charges in the injection valves to ensure proper operation will occur if required. Other administrative controls, such as those that limit the shelf life of the explosive charges, must be followed. The 31 day Frequency is based on operating experience that has demonstrated the reliability of the explosive charge continuity.

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 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.

SR 3.1.7.4 is modified by a Note that states that SR is not required to be met for one squib charge intermittently bypassed under administrative controls. This is acceptable because a keylock bypass may be used on one of the two squibs for each valve without rendering the valve inoperable.

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 tank. SR 3.1.7.6 must be performed any time boron or water is added to the accumulator tank 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 92 day Frequency of this Surveillance is appropriate because the boron solution is not expected to change concentration between surveillances.

The plant design ensures that neither evaporation nor condensation of water vapor will occur in the high pressure SLC accumulator tank during plant power operation. Maintenance of the design ambient temperature of the SLC equipment room, tank, piping and valves ameliorates any tendency for the sodium pentaborate to ever go out of solution, thus, mixing and sampling the accumulator tank volume every 92 days is a conservative approach to establishing the continued system OPERABILTY including verification of the flow path from the accumulator to the squib valves. This also conserves the concentrated, highly enriched sodium pentaborate to allow optimum sampling volumes during the operating cycle without the need to depressurize and refill the accumulator tank. Replenishment should only need to be done during refueling outages when the system is normally out of service.

BASES

SR 3.1.7.7

The SLC trains are required to actuate automatically to perform their design function. This Surveillance test verifies that, with a required system initiation signal (actual or simulated), the mechanical portions of the SLC operates as designed when initiated either by an actual or simulated initiation signal, causing proper actuation of all the required components. The LOGIC SYSTEM FUNCTIONAL TEST performed in LCO 3.3.1.8 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 Frequency was concluded to be acceptable from a reliability standpoint.

This SR is modified by a Note that excludes squib valve actuation. This is acceptable because the valve actuation is verified by SR 3.1.7.8.

SR 3.1.7.8

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 tank to ensure that the proper B-10 atom percent is being used.

REFERENCES

1. 10 CFR 50.62
2. Section 9.3.5.
3. Section 7.8.1.1

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 100. 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 MCPR 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

	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	<u>A.1</u> 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. <u>B.1</u> 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	<u>SR 3.2.3.1</u> 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

BASES

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-0800, Standard Review Plan 4.2, “Fuel System Design,” Section II A.2(g), Revision 2, July 1981.

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 MCPR Safety Limit (SL) is set such that 99.9% of the fuel rods avoid boiling transition if the limit is not violated (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 MCPR SL is not exceeded during any transient event that occurs with moderate frequency, limiting transients have been analyzed to determine the largest reduction in critical power ratio (CPR). The types of transients evaluated are loss of feedwater flow, increase in pressure and power, positive reactivity insertion, and coolant temperature decrease. The limiting transient yields the largest change in CPR (ΔCPR). When the largest ΔCPR is added to the MCPR SL, the required operating limit MCPR is obtained.

The MCPR operating limits derived from the transient analysis are dependent on the power state ($MCPR_p$) to ensure adherence to fuel design limits during the worst transient that occurs with moderate frequency.

Power-dependent MCPR limits ($MCPR_p$) are determined for the anticipated transients that are significantly affected by power.

BASES

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 ratio is very small. Surveillance of thermal limits below [25%] RTP is unnecessary due to the large inherent margin that ensures that the MCPR SL is not exceeded even if a limiting transient occurs.

Statistical analyses documented in Reference 2 indicate that the nominal value of the initial MCPR expected at [25%] RTP is > 3.5. 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. This trend is expected to continue to the 5% to 15% power range when entry into MODE 2 occurs. 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.

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

BASES

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. “BWR/6 Generic Rod Withdrawal Error Analysis,” Appendix 15B, General Electric Standard Safety Analysis Report (GESSAR-II).

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...so chosen that automatic protective action will correct the abnormal situation before a Safety Limit (SL) is exceeded." The Analytic Limit is the limit of the process variable at which a safety action is initiated, as established by the safety analysis, to ensure that a SL is not exceeded. Any automatic protection action that occurs on reaching the Analytic Limit therefore ensures that the SL is not exceeded. However, in practice, the actual settings for automatic protective devices must be chosen to be more conservative than the Analytic Limit to account for instrument loop uncertainties related to the setting at which the automatic protective action would actually occur.

The trip setpoint is a predetermined setting for a protective device chosen to ensure automatic actuation prior to the process variable reaching the Analytic Limit and thus ensuring that the SL would not be exceeded. As such, the trip setpoint accounts for uncertainties in setting the device (e.g., calibration), uncertainties in how the device might actually perform (e.g., repeatability), changes in the point of action of the device over time (e.g., drift during surveillance intervals), and any other factors that may influence its actual performance (e.g., harsh accident environments). In this manner, the trip setpoint plays an important role in ensuring that SLs are not exceeded. As such, the trip setpoint meets the definition of an LSSS and could be used to meet the requirement that they be contained in the Technical Specifications.

Technical Specifications contain values related to the OPERABILITY of equipment required for safe operation of the facility. OPERABLE is defined in Technical Specifications as "...being capable of performing its safety function(s)." For automatic protective devices, the required safety function is to ensure that a SL is not exceeded and therefore the LSSS as defined by 10 CFR 50.36 is the same as the OPERABILITY limit for these devices. However, use of the trip setpoint to define OPERABILITY in Technical Specifications and its corresponding designation as the LSSS required by 10 CFR 50.36 would be an overly restrictive requirement if it were applied as an OPERABILITY limit for the "as found" value of a protective device setting during a Surveillance. This would result in Technical Specification compliance problems, as well as reports and corrective actions required by the rule that are not necessary to ensure safety. For example, an automatic protective device with a setting that has been found to be different from the trip setpoint due to some drift of the setting may still be OPERABLE since drift is to be expected. This expected drift would have been specifically accounted for in the setpoint methodology for calculating the trip setpoint and thus the automatic protective action would still have ensured that the SL would not be exceeded with the "as found" setting of the protective device. Therefore, the device would still be OPERABLE since it would have performed its safety function and the only corrective action required would be to reset the device to the trip setpoint to account for further drift during the next surveillance interval.

Use of the trip setpoint to define "as found" OPERABILITY and its designation as the LSSS under the expected circumstances described above would result in actions required by both the rule and Technical Specifications that are clearly not warranted. However, there is also some point beyond which the device would have not been able to perform its function due, for example, to greater than expected drift. This value needs to be specified in the Technical Specifications in order to define OPERABILITY of the devices and is designated as the Allowable Value which, as stated above, is the same as the LSSS.

The Allowable Valuable specified in Table 3.3.1-1 serves as the LSSS such that a channel is OPERABLE if the trip setpoint is found not to exceed the Allowable Value. As such, the Allowable Value differs from the trip setpoint by an amount primarily equal to the expected instrument loop uncertainties, such as drift, during the surveillance interval. In this manner, the actual setting of the device will still meet the LSSS definition and ensure that a SL is not exceeded at any given point of time as long as the device has not drifted beyond that expected during the surveillance interval. If the actual setting of the device is found to have exceeded the Allowable Value the device would be considered inoperable from a Technical Specification perspective. This requires corrective action including those actions required by 10 CFR 50.36 when automatic protective devices do not function as required. Note that, although the channel is "OPERABLE" under these circumstances, the trip setpoint should be left adjusted to a value within the established trip setpoint calibration tolerance band, in accordance with uncertainty assumptions stated in the referenced setpoint methodology (as-left criteria), and confirmed to be operating within the statistical allowances of the uncertainty terms assigned. The LSSS is defined in this Specification as the Allowable Value, which in conjunction with the LCOs, establish the threshold for protective system action to prevent exceeding acceptable limits including Safety Limits during Design Basis Accidents (DBAs).

The RPS, as shown in Reference 1, includes sensors, digital trip modules (DTMs), trip logic units (TLUs), load drivers (LDs), bypass circuits, and switches that are necessary to cause initiation of a reactor scram. 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, control rod drive 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. There are at least four redundant sensor input signals from each of these parameters (with the exception of manual scram). Most channels include electronic equipment (e.g., DTMs) that compares measured input signals with pre-established setpoints. When the setpoint is exceeded, the DTM outputs an RPS trip signal to the trip logic.

The RPS has digitally multiplexed analog process variables inputs to the two-out-of-four trip input initiation logic. Other inputs such as MSIV position scram inputs are hardwired to the RPS. Four separate instrument divisions are used to monitor the required variables. Four separate divisions of trip logic are then used to perform the required trip determination. This occurs within the divisional Digital Trip Modules (DTMs). An exception to this approach are inputs from the Neutron Monitoring System (NMS), which is discussed below. Each divisional DTM receives input from the instrumentation in that same division for each variable monitored. For analog variables the DTMs make the 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. For some variables trip determinations are made by the monitoring element itself (e.g., limit switch). In such cases the DTM simply passes on the signal in the form of a trip/no-trip output. The output of each divisional DTM (a trip/no-trip condition) for each variable is then routed to all four divisional Trip Logic Units (TLUs) such that each divisional TLU receives input from each of the four divisions of DTMs.

For maintenance purposes and added reliability, each DTM has a division-of-sensors bypass such that all instruments in that division will be bypassed in the RPS trip logic at the TLUs. 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.

All average power range monitors (APRM) and and startup range neutron monitors (SRNM) trip decisions are made within the NMS. This is done on a divisional basis and the results then sent directly to the RPS TLUs (i.e., the DTM function is done within the NMS). Thus, each NMS division sends only two inputs to the RPS divisional TLUs, one for APRM trip/no-trip and one for SRNM trip/no-trip. A divisional APRM 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 tripped or SRNM tripped basis, by looking at the four divisions of APRM and four divisions of SRNM. All bypasses of the SRNMs and APRMs are performed within and by the NMS.

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 Output Logic Unit (OLU). It is this trip that then initiates a reactor scram by tripping load drivers in the power circuits that energize the CRD scram pilot valve solenoids. Each OLU sends output signals to a total of eight load drivers, four each associated with the ‘A’ and ‘B’ scram pilot valve solenoids, respectively. The total set of 32 load drivers are grouped in a series-parallel arrangement such that each load driver group energizes either the ‘A’ or the ‘B’ scram pilot valve solenoids for the control rods in one of four distinct groups of control rods. 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 cause the de-energization of both the ‘A’ and ‘B’ scram pilot valve solenoids for all four groups of control rods, affecting a full reactor scram. Each of the four TLUs has a bypass switch so that they can be bypassed, only one at any one time, such that the RPS 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 scram. Each OLU has test and trip switches such that the load drivers can be tested both with and without causing a half scram condition (i.e., tripping of either the ‘A’ or ‘B’ scram pilot valve solenoids).

Manual scram is accomplished either via two manual scram push buttons or by placing the reactor mode switch in the shutdown position. Both manual scram functions directly interrupt power in the circuits that energize the scram pilot valve solenoids such that a full scram results. This occurs upstream of the load driver groups and is completely separate from the associated automatic scram logic. They are also hardwired and therefore not reliant on the plant multiplexing system. 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 coincidentally 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.

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 the nominal setpoints that are derived from Allowable Values specified by the setpoint methodology and listed in Table 3.3.1.1-1 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 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 instrumentation channel Functions specified in Table 3.3.1.1-1. Each Function must have the required number of OPERABLE channels, with their setpoints within the specified Allowable Value, where appropriate. The actual setpoint is calibrated consistent with applicable setpoint methodology assumptions. Each channel must also respond within its assumed response time.

Allowable Values are specified for each RPS Function specified in the Table. Nominal trip setpoints are specified in the setpoint calculations. The nominal setpoints are selected to ensure the actual setpoints do not exceed the Allowable Value between successive CHANNEL CALIBRATIONS. Operation with a trip setpoint less conservative than the nominal trip setpoint, but within its Allowable Value, is acceptable. A channel is inoperable if its actual trip setpoint is not within its required Allowable Value.

Trip setpoints 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, the associated device (e.g., digital trip module) changes state. The analytic limits are derived from the limiting values of the process parameters obtained from the safety analysis. [The Allowable Values are derived from the analytic limits, corrected for calibration, process and some of the instrument errors. The trip setpoints 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 channels that must function in harsh environments as defined by 10 CFR 50.49) are accounted for.

The OPERABILITY of 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 are required in each MODE to provide primary and diverse initiation signals.

BASES

RPS is required to be OPERABLE in MODE 6 with any control rod withdrawn from a core cell containing one or more fuel assemblies. 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) and rod-out/rod pair interlock (LCO 3.9.2) ensure no event requiring RPS will occur. 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]) does not allow any control rod to be withdrawn. 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.

1. Startup Range Neutron Monitors (SRNMs)

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, "Nuclear Monitoring (NMS) Instrumentation." The SRNM provides diverse protection for the Rod Worth Minimizer (RWM) in the 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.

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

Three channels of SRNM 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. Average Power Range Monitors (APRMs)

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

Three channels of APRMs 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 Functions are required (LCO 3.3.1.4).

3. Control Rod Drive (CRD) Accumulator Charging Water Header Pressure - Low

To maintain the continuous ability to scram, the 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 charging water header. Pressure in the charging water header is monitored. The CRD Accumulator Charging Water Header Pressure - Low Function initiates a scram if a significant degradation in the 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.

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

Three channels of CRD Accumulator Charging Water Header Pressure - 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. 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 reactor scram terminates the load rejection/turbine trip events and along with the safety/relief valves limits the peak RPV pressure to less than the ASME Section III Code limits.]

High reactor pressure signals are initiated from four pressure transmitters 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.

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 in the analysis of loss of feedwater (Ref. 4). The reactor scram reduces the amount of energy required to be absorbed and, along with the actions of the Emergency Core Cooling System (ECCS), 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 level transmitters 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 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.

The Reactor Vessel Water Level - Low, Level 3 Allowable Value is selected to ensure that for transients involving loss of all normal feedwater flow, initiation of the ECCS systems at RPV Water Level 1 will not be required.

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 that MCPR is maintained above the MCPR Safety Limit. The Reactor Vessel Water Level - High, Level 8, Function is one of the many Functions assumed to be OPERABLE and capable of providing a reactor scram during transients analyzed in Reference 2. It is directly assumed in the analysis of feedwater controller failure, maximum demand (Ref. 5).

Reactor Vessel Water Level - High, Level 8, signals are initiated from four level transmitters 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 MCPR Safety Limit is not violated during the assumed transient.

Three channels of the Reactor Vessel Water Level - High, Level 8, arranged in a two-out-of-four logic are available and 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

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. MSIV closure is assumed in the transients analyzed in References 6 and 7, (e.g., low steam line pressure, manual closure of MSIVs, [high steam line flow]). 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 fuel peak cladding temperature remains below the limits of 10 CFR 50.46.

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 isolation valve and two position switches are mounted on the outboard isolation valve. Each of the two position switches on any one MSL isolation valve 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.

The MSIV - Closure (per Steam Line) 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 MSIV - Closure Function (per Steam Line) 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 a secondary scram signal to Reactor Vessel Water Level - Low, Level 3, for LOCA events inside the drywell. 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.

High drywell pressure signals are initiated from four pressure transmitters that sense drywell pressure. The Allowable Value was selected to be as low as possible and be indicative of a LOCA inside primary containment.

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 Average Temperature - High

High temperature in the suppression pool could indicate a break in the RCS pressure boundary or a leak through the safety/relief valves (S/RVs), or stuck open S/RV(s). 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 or stuck opened S/RV or depressurization valve References 8, 9, and 10.

High suppression pool temperature signals are initiated from four divisions of temperature sensors located in the suppression pool. The Allowable Value was selected considering the maximum operating temperature and to be indicative of an inadvertent open S/RV. Four channels of Class 1E 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 E dCIS, which in turn provides the equivalent digital signal to the appropriate DTM. The temperature sensors and associated instrument lines are components of the 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.]

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

10. Turbine Stop Valve (TSV) Closure

Closure of the TSVs 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. The Turbine Stop Valve (TSV) Closure Function is the primary scram signal for the turbine trip event analyzed in Reference 11. For this event, the reactor scram reduces the amount of energy required to be absorbed and ensures that the MCPR SL is not exceeded.

BASES

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 open/close contact output signal through hard-wired connection to the SSLC DTM in one of the four RPS sensor channels. The logic for the Turbine Stop Valve Closure Function is such that [three or more] TSVs must be closed to produce a scram.

The Function is enabled at THERMAL POWER ≥ [40]% RTP. This is accomplish automatically by [pressure transmitter sensing turbine first stage pressure transmitters].

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.

This RPS scram is automatically bypassed if sufficient number of the bypass valves is opening as indicated by their 10% position sensors within a preset time delay after the initiation of the reactor trip signal caused by the TCV fast closure. The bypass is automatically removed the scram trip function enabled at a THERMAL POWER above the bypass setpoint.

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

Fast closure of the 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. 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 12. For this event, the reactor scram reduces the amount of energy required to be absorbed and ensures that the MCPR SL is not exceeded.

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 transmitter associated with each control valve. Each pressure transmitter provides a signal through hard wired connections to the SSLC DTM in each of the four RPS sensor channels. This Function must be enabled at THERMAL POWER ≥ [40]% RTP. This is normally accomplished automatically by pressure transmitters sensing turbine first stage pressure.

The Function is enabled at THERMAL POWER ≥ [40]% RTP. This is accomplish automatically by [pressure transmitter sensing turbine first stage pressure transmitters].

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.

This RPS scram is automatically bypassed if sufficient number of the bypass valves is opening as indicated by their 10% position sensors within a preset time delay after the initiation of the reactor trip signal caused by the TCV fast closure. The bypass is automatically removed the scram trip function enabled at a THERMAL POWER above the bypass setpoint.

12. Main Condenser Vacuum - Low

The Main Condenser Pressure—Low Function is provided to shut down the reactor and reduce the energy input to the main condenser to help prevent overpressurization of the main condenser in the event of a loss of the main condenser vacuum. The Main Condenser Pressure - Low Function is the primary scram signal for the loss of condenser vacuum event analyzed in Reference 13. For this event, the reactor scram reduces the amount of energy required to be absorbed by the main condenser and helps to ensure the MCPR SL is not exceeded by reducing the core energy prior to the fast closure of the turbine stop valves. This Function helps maintain the main condenser as a heat sink during this event. The reactor scram at Main Condenser Pressure - Low 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.

Main Condenser Pressure signals are derived from four pressure switches that sense the pressure in the condenser. Each pressure transmitter provides an analog output signal through hard-wired connections to the SSLC 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—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. [The Function is required in MODE 1 since, in this MODE, a significant amount of core energy can be rejected to the main condenser. During MODE 2, 3, 4, 5, and 6, the core energy is significantly lower.]

<u>13. Loss of Power Generation Bus (Loss of Feedwater Flow</u>)

The plant electrical system has four redundant power generation busses that operate at 13.8 kV. These busses supply power for the feedwater pumps and other pumps. In MODE 1, at least three of the four busses must be powered. 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 2-out-of-4 logic will initiate a scram after a preset delay time. This delay time is to accommodate for the fast transfer from the UAT transformer feed to the RAT transformer feed. When the power generation busses 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.

Loss of Power Generation Bus signals are derived from four voltage sensors. A 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 2-out-of-4 logic will initiate a scram after a preset delay time. The Allowable Value was selected high

BASES

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 Loss of Power Generation Bus 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. Oscillation Power Range Monitors (OPRMs)

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

Three channels of OPRMs 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 OPRMs Functions are required (LCO 3.3.1.4).

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.

A.1

With one or more Function with one or more required RPS instrumentation channels inoperable, the affected instrument division must be placed in trip. Because of the diversity of sensors available to provide trip signals and the redundancy of the RPS design, an allowable out of service time of 12 hours is considered acceptable to permit restoration of any inoperable channel to OPERABLE status. However, this out of service time is only acceptable provided the associated

Function still maintains RPS trip capability (refer to Required Actions B.1 Bases). If the inoperable channel cannot be restored to OPERABLE status within the allowable out of service time, the affected instrument division must be placed in trip. Placing the RPS division in trip would conservatively compensate for the inoperability and allow operation to continue. Alternately, if it is not desired to place the RPS division in trip (e.g., as in the case where placing the RPS division in trip would result in a full scram), Condition C must be entered and its Required Action taken. Most repairs are likely to be simple card or other electronic subassembly replacements that can be done on-line with the affected division of sensors in bypass. In such cases, restoration should be done as soon as practicable.

B.1

Required Action B.1 is intended to ensure that appropriate actions are taken if multiple, inoperable, untripped channels (i.e., three or more channels for most Function) 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. For the typical Function with two-out-of-four logic, this would require two channels to be OPERABLE or in trip (instrument division in trip). For Function 7 (Main Steam Isolation Valve - Closure (Per Steam Line), this would require the logic to have each channel associated with the MSIVs in three MSLs (not necessarily the same MSLs), OPERABLE or in trip (instrument division in trip).

The Completion Time is intended to allow the operator time to evaluate and repair any discovered inoperabilities. The 1 hour Completion Time is acceptable because it minimizes risk while allowing time for restoration or tripping of channels.

C.1

Required Action C.1 directs entry into the appropriate Condition referenced in Table 3.3.1.1-1. 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. Each time an inoperable channel has not met any Required Action of Condition A or B, and the associated Completion Time has expired, Condition C will be entered for that channel and provides for transfer to the appropriate subsequent Condition.

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

If the channel(s) is not restored to OPERABLE status, or the division of sensors are not placed in bypass or if the instrument division is not placed in trip, 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. In addition, the Completion Time of Required Action D.1 and E.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.

The Surveillances are modified by a Note to indicate that a 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 or up to 6 hours provided the associated Function maintains trip capability. Upon completion of the Surveillance, or expiration of the 6 hour allowance, the channel must be returned to OPERABLE status or the applicable Condition entered and Required Actions taken. This Note is based on the assumption that 6 hours is the average time required to perform channel surveillance. The 6 hour testing allowance does not significantly reduce the probability that the RPS will trip when necessary.

SR 3.3.1.1.1

Performance of the CHANNEL CHECK once every 24 hours ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the parameter indicated on one channel to a similar parameter on other channels. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value. Significant deviations between the instrument channels could be an indication of excessive instrument drift in one of the channels or something even more serious. A CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

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

The Frequency is based upon 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 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. Any setpoint adjustment shall be consistent with the assumptions of the current plant specific setpoint methodology.

The Frequency of [184 days] is based on the reliability of the channels and the self monitoring capability of the RPS System.

SR 3.3.1.1.3

A CHANNEL CALIBRATION is a complete check of the instrument loop and the sensor. This test verifies the channel responds to the measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drifts between successive calibrations consistent with the plant specific setpoint methodology.

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 3.3.1.1.4

This SR ensures that the individual channel response times are less than or equal to the maximum values assumed in the accident analysis.

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

RPS RESPONSE TIME tests are conducted on a 24 month on a STAGGERED TEST BASIS. Therefore, staggered testing results in response time verification of these devices every 24 months. The

BASES

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

REFERENCES

1. Figure 7.2-1.
2. Chapter 15.
3. Section 7.7.
4. Section 15.2.
5. Section 15.3.
6. Section 15.3.
7. Section 15.2.
8. Section 15.3.
9. Section 15.3.
10. Section 15.3.
11. Section 15.2.
12. Section 15.2.
13. 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 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...so chosen that automatic protective action will correct the abnormal situation before a Safety Limit (SL) is exceeded." The Analytic Limit is the limit of the process variable at which a safety action is initiated, as established by the safety analysis, to ensure that a SL is not exceeded. Any automatic protection action that occurs on reaching the Analytic Limit therefore ensures that the SL is not exceeded. However, in practice, the actual settings for automatic protective devices must be chosen to be more conservative than the Analytic Limit to account for instrument loop uncertainties related to the setting at which the automatic protective action would actually occur.

The RPS, as shown in Reference 1, includes sensors, digital trip modules (DTMs), trip logic units (TLUs), load drivers (LDs), bypass circuits, and switches that are necessary to cause initiation of a reactor scram. 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, control rod drive 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 input parameters to RPS are covered in LCO 3.3.1.1, “Reactor Protection System (RPS) Instrumentation” and the nuclear instrumentation is covered in LCO 3.3.1.4.

BASES

The RPS has digitally multiplexed analog process variables inputs to the two-out–of–four trip input initiation logic. Other inputs such as MSIV position scram inputs are hardwired to the RPS. Four separate instrument divisions are used to monitor the required variables. Four separate divisions of trip logic are then used to perform the required trip determination. This occurs within the divisional Digital Trip Modules (DTMs). An exception to this approach are inputs from the Neutron Monitoring System (NMS), which is discussed below. Each divisional DTM receives input from the instrumentation in that same division for each variable monitored. For analog variables the DTMs make the 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. For some variables trip determinations are made by the monitoring element itself (e.g., limit switch). In such cases the DTM simply passes on the signal in the form of a trip/no-trip output. The output of each divisional DTM (a trip/no-trip condition) for each variable is then routed to all four divisional Trip Logic Units (TLUs) such that each divisional TLU receives input from each of the four divisions of DTMs.

For maintenance purposes and added reliability, each DTM has a division of sensors bypass such that all instruments in that division will be bypassed in the RPS trip logic at the TLUs. 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.

All average power range monitors (APRM) and startup range neutron monitors (SRNM) trip decisions are made within the NMS. This is done on a divisional basis and the results then sent directly to the RPS TLUs (i.e., the DTM function is done within the NMS). Thus, each NMS division sends only two inputs to the RPS divisional TLUs, one for APRM trip/no-trip and one for SRNM trip/no-trip. A divisional APRM 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 tripped or SRNM tripped basis, by looking at the four divisions of APRM and four divisions of SRNM. All bypasses of the SRNMs and APRMs are performed within and by the NMS. The NMS Instrumentation is covered in LCO 3.3.1.4.

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 exceeds the value in two instrument divisions for the same variable 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

BASES

causes a trip in its corresponding Output Logic Unit (OLU). It is this trip that then initiates a reactor scram by tripping load drivers in the power circuits that energize the CRD scram pilot valve solenoids. Each OLU sends output signals to a total of eight load drivers, four each associated with the ‘A’ and ‘B’ scram pilot valve solenoids, respectively. The total set of 32 load drivers are grouped in a series-parallel arrangement such that each load driver group energizes either the ‘A’ or the ‘B’ scram pilot valve solenoids for the control rods in one of four distinct groups of control rods. 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 cause the de-energization of both the ‘A’ and ‘B’ scram pilot valve solenoids for all four groups of control rods, affecting a full reactor scram. Each of the four TLUs has a bypass switch so that they can be bypassed, only one at any one time, such that the RPS 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 scram. Each OLU has test and trip switches such that the load drivers can be tested both with and without causing a half scram condition (i.e., tripping of either the ‘A’ or ‘B’ scram pilot valve solenoids).

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.

This Specification covers the RPS actuation circuitry that covers the TLUs, RPS OLUs, and the LDs.

APPLICABLE SAFETY ANALYSES

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 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 channels support the OPERABILITY of the RPS Instrumentation, “LCO 3.3.1.1, Reactor Protection System (RPS)

BASES

Instrumentation" and therefore is required to be OPERABLE. This Specification covers the RPS actuation circuitry which covers the TLUs, RPS OLUs, and the LDs.

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

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

LCO

Four RPS automatic actuation channels are required to be OPERABLE to ensure no single automatic actuation channel failure will preclude a scram to occur on a valid signal. This Specification covers the RPS actuation circuitry which covers the TLUs, RPS OLUs, and the LDs.

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

APPLICABILITY

The four RPS automatic actuation channels 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. In MODES 1 and 2, the control rods are assumed to function during a DBA or transient and therefore the four RPS automatic actuation channels are required to be OPERABLE in these MODES. In MODES 3, 4, and 5, control rods can not be withdrawn since the reactor mode switch is in shutdown and a control rod block is applied. Therefore, RPS automatic actuation is not required to be OPERABE in these MODES.

ACTIONS

A Note has been provided to modify the ACTIONS related to RPS automatic actuation 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 automatic actuation 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 automatic actuation channel.

A.1

Because of the redundancy of RPS automatic actuation channels available, an allowable out of service time of 12 hours is considered an acceptable to permit restoration of any required inoperable channel to OPERABLE status. However, this out of service time is only acceptable provided there is only one required inoperable RPS automatic actuation channel still maintains RPS trip capability (refer to Required Action B.1 Bases). If the inoperable channel cannot be restored to OPERABLE status within the allowable out of service time, the affected actuation division must be placed in trip. This is acceptable because the capability to accommodate a single failure exists and the reliability of the RPS automatic actuation logic. Placing the actuation division in trip would conservatively compensate for the inoperability, restore capability to accommodate a single failure, and allow operation to continue. Alternately, if it is not desired to place actuation division in trip (e.g., as in the case where placing the inoperable channel in trip would result in a full scram), Condition C must be entered and it's Required Action taken.

B.1

Condition B exists when one or more Functions have two or more required RPS automatic actuation channels inoperable. Required Action B.1 is intended to ensure that appropriate actions are taken if multiple, inoperable, untripped channels (i.e., two or more required channels) result in the Function not maintaining NMS trip capability. A Function is considered to be maintaining NMS trip capability when sufficient channels 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 RPS automatic actuation channels, two channels must be OPERABLE or in trip to maintain RPS trip capability.

The Completion Time is intended to allow the operator time to evaluate and repair any discovered inoperabilities. The 1 hour Completion Time is acceptable because it minimizes risk while allowing time for restoration or tripping of channels. Alternately, if it is not desired to place actuation division in trip (e.g., as in the case where placing the inoperable channel in trip would result in a full scram), Condition C or D must be entered, as applicable and it's Required Action taken.

BASES

C.1

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 are 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

D.1

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

The Surveillances are modified by a Note to indicate that a 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 or up to 6 hours provided the associated Function maintains trip capability. Upon completion of the Surveillance, or expiration of the 6 hour allowance, the channel must be returned to OPERABLE status or the applicable Condition entered and Required Actions taken. This Note is based on the assumption that 6 hours is the average time required to perform channel surveillance. The 6 hour testing allowance does not significantly reduce the probability that the RPS will trip when necessary.

SR 3.3.1.2.1

The LOGIC SYSTEM FUNCTIONAL TEST demonstrates the OPERABILITY of the RPS Actuation channels, including the TLUs, RPS OLUs, and LDs for a specific channel. The functional testing of control rods, in LCO 3.1.3, overlaps this Surveillance to provide complete testing of the assumed safety function.

BASES

REFERENCES

1. Chapter 7, Figure 7.2-1.
2. Chapter 15.

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 (Division 1 and Division 2 Reactor Mode Switch – Shutdown actuation channels). Both manual scram functions directly interrupt power in the circuits that energize the scram pilot valve solenoids such that a full scram results. This occurs upstream of the load driver groups and is completely separate from the associated automatic scram logic. They are also hardwired and therefore not reliant on the plant multiplexing system. 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 coincidentally 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.

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.] The OPERABILITY of scram pilot valves and associated solenoids, and backup scram valves, described in the Background section, are not addressed by this LCO.
LCO	The Division 1 and Division 2 manual actuation channels and Division 1 and 2 Reactor Mode Switch – Shutdown actuation channels are required to be OPERABLE to retain the overall redundancy and diversity of the RPS.
APPLICABILITY	The two RPS manual actuation channels 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. In MODES 1 and 2, the control rods are assumed to function during a DBA or transient and therefore the four RPS manual actuation channels are required to be OPERABLE in these MODES. In MODES 3, 4, and 5, control rods cannot be withdrawn since the reactor mode switch is in shutdown and a control rod block is applied. Therefore, RPS manual actuation channel are not required to be OPERABE in these MODES.
ACTIONS	A Note has been provided to modify the ACTIONS related to RPS manual actuation 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 manual actuation 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. <u>A.1</u> If either the Division 1 or Division 2 manual actuation channel inoperable inoperable the capability to shutdown the unit with the manual actuation channels is lost. If the Division 1 and Division 2 Reactor Mode Switch -

BASES

Shutdown actuation channels are inoperable the manual trip capability with these channels is lost. Required Action C.1 is intended to ensure that appropriate actions are taken to ensure manual trip capability is maintained for the inoperable Function. RPS manual actuation capability is maintained when sufficient channels are OPERABLE or in trip such that the RPS logic will generate a trip signal from the given Function. This would require two RPS manual actuation channels to be OPERABLE or in trip.

The Completion Time is intended to allow the operator time to evaluate and repair any discovered inoperabilities. The [1] hour Completion Time is acceptable because it minimizes risk while allowing time for restoration or tripping of channels.

B.1

If any Required Action and associated Completion Time of Condition A 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 are 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

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 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

The Surveillances are modified by a Note to indicate that a 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 or up to 6 hours provided the associated Function maintains trip capability. Upon completion of the Surveillance, or expiration of the 6 hour allowance, the channel must be returned to OPERABLE status or the applicable Condition entered and Required Actions taken. This Note is based on the assumption that 6 hours is the average time required to perform channel surveillance. The 6 hour

BASES

testing allowance does not significantly reduce the probability that the RPS will trip when necessary.

SR 3.3.1.3.1

A CHANNEL FUNCTIONAL TEST is performed on the manual actuation channels to ensure that the channels will perform the intended Function. A Frequency of [92] days is considered to be acceptable.

SR 3.3.1.3.2

The LOGIC SYSTEM FUNCTIONAL TEST (LSFT) demonstrates the OPERABILITY of the required trip logic for the manual actuation channels and the Reactor MODE Switch – Shutdown Position actuation channels. The functional testing of control rods (LCO 3.1.3, “Control Rod Operability” 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. 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). This can be accomplished either automatically or manually.

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...so chosen that automatic protective action will correct the abnormal situation before a Safety Limit (SL) is exceeded." The Analytic Limit is the limit of the process variable at which a safety action is initiated, as established by the safety analysis, to ensure that a SL is not exceeded. Any automatic protection action that occurs on reaching the Analytic Limit therefore ensures that the SL is not exceeded. However, in practice, the actual settings for automatic protective devices must be chosen to be more conservative than the Analytic Limit to account for instrument loop uncertainties related to the setting at which the automatic protective action would actually occur.

The trip setpoint is a predetermined setting for a protective device chosen to ensure automatic actuation prior to the process variable reaching the Analytic Limit and thus ensuring that the SL would not be exceeded. As such, the trip setpoint accounts for uncertainties in setting the device (e.g., calibration), uncertainties in how the device might actually perform (e.g., repeatability), changes in the point of action of the device over time (e.g., drift during surveillance intervals), and any other factors which may influence its actual performance (e.g., harsh accident environments). In this manner, the trip setpoint plays an important role in ensuring that SLs are not exceeded. As such, the trip setpoint meets the definition of an LSSS and could be used to meet the requirement that they be contained in the Technical Specifications.

BASES

Technical Specifications contain values related to the OPERABILITY of equipment required for safe operation of the facility. OPERABLE is defined in Technical Specifications as "...being capable of performing its safety function(s)." For automatic protective devices, the required safety function is to ensure that a SL is not exceeded and therefore the LSSS as defined by 10 CFR 50.36 is the same as the OPERABILITY limit for these devices. However, use of the trip setpoint to define OPERABILITY in Technical Specifications and its corresponding designation as the LSSS required by 10 CFR 50.36 would be an overly restrictive requirement if it were applied as an OPERABILITY limit for the "as found" value of a protective device setting during a Surveillance. This would result in Technical Specification compliance problems, as well as reports and corrective actions required by the rule which are not necessary to ensure safety. For example, an automatic protective device with a setting that has been found to be different from the trip setpoint due to some drift of the setting may still be OPERABLE since drift is to be expected. This expected drift would have been specifically accounted for in the setpoint methodology for calculating the trip setpoint and thus the automatic protective action would still have ensured that the SL would not be exceeded with the "as found" setting of the protective device. Therefore, the device would still be OPERABLE since it would have performed its safety function and the only corrective action required would be to reset the device to the trip setpoint to account for further drift during the next surveillance interval.

Use of the trip setpoint to define "as found" OPERABILITY and its designation as the LSSS under the expected circumstances described above would result in actions required by both the rule and Technical Specifications that are clearly not warranted. However, there is also some point beyond which the device would have not been able to perform its function due, for example, to greater than expected drift. This value needs to be specified in the Technical Specifications in order to define OPERABILITY of the devices and is designated as the Allowable Value which, as stated above, is the same as the LSSS.

The Allowable Valuable specified in Table 3.3.1-1 serves as the LSSS such that a channel is OPERABLE if the trip setpoint is found not to exceed the Allowable Value. As such, the Allowable Value differs from the trip setpoint by an amount primarily equal to the expected instrument loop uncertainties, such as drift, during the surveillance interval. In this manner, the actual setting of the device will still meet the LSSS definition and ensure that a SL is not exceeded at any given point of time as long as the device has not drifted beyond that expected during the surveillance interval. If the actual setting of the device is found to have exceeded the Allowable Value the device would be considered inoperable from a

BASES

Technical Specification perspective. This requires corrective action including those actions required by 10 CFR 50.36 when automatic protective devices do not function as required. Note that, although the channel is "OPERABLE" under these circumstances, the trip setpoint should be left adjusted to a value within the established trip setpoint calibration tolerance band, in accordance with uncertainty assumptions stated in the referenced setpoint methodology (as-left criteria), and confirmed to be operating within the statistical allowances of the uncertainty terms assigned. The LSSS is defined in this Specification as the Allowable Value, which in conjunction with the LCOs, establish the threshold for protective system action to prevent exceeding acceptable limits including Safety Limits during Design Basis Accidents (DBAs).

The NMS is composed of the startup range neutron monitor (SRNM) and the average power range monitor (APRM). Separate, isolated, digital Startup Range Neutron Monitor (SRNM) trip signal and Average Power Range Monitor (APRM) trip signal 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 upscale (high count rate or high flux level); Short (fast) period; and SRNM inoperative. The three 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.

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 (upscale, or inoperative, or short period) will result in an SRNM division trip. Each SRNM divisional output is provided to each of the four divisions (SRNM interface unit). The SRNM interface 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. One channel from each bypass group may be bypassed from the operator’s control console. Thus, up to four channels may be bypassed at any one time. There is no additional SRNM bypass

BASES

capability at the divisional level, however, it is possible to bypass all of the SRNMs within a division.

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 high neutron flux, high simulated thermal power, and APRM inoperative.

There are four APRM channels divided into four NMS divisions. For each division, any one APRM channel trip (upscale or inoperative) will result in a division trip. Each APRM divisional output is provided to each of the four divisions (APRM interface unit). The SPRM interface unit determines whether there are sufficient SRNM divisions in trip (two-out-of-four logic). One APRM channel from may be bypassed at any one time.

The APRMs 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 and one for SRNM trip/no-trip. A divisional APRM 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 tripped or SRNM tripped basis, by looking at the four divisions of APRM and four divisions of SRNM. All bypasses of the SRNMs and APRMs are performed within and by the NMS.

This Specification covers the SRNM channel from the sensor to the NMS divisional interface unit and up to each of the SRNM interface units. LCO 3.3.1.5, covers NMS automatic actuation.

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

The actions of the NMS in conjunction with RPS are assumed in the safety analyses of Reference 2. The RPS initiates a reactor scram when monitored parameter values exceed the nominal setpoints that are derived from Allowable Values specified by the setpoint methodology and listed in Table 3.3.1.4 -1 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 within the specified Allowable Value, where appropriate. The actual setpoint is calibrated consistent with applicable setpoint methodology assumptions. Each channel must also respond within its assumed response time.

Allowable Values are specified for each RPS Function specified in the Table. Nominal trip setpoints are specified in the setpoint calculations. The nominal setpoints are selected to ensure the actual setpoints do not exceed the Allowable Value between successive CHANNEL CALIBRATIONS. Operation with a trip setpoint less conservative than the nominal trip setpoint, but within its Allowable Value, is acceptable. A channel is inoperable if its actual trip setpoint is not within its required Allowable Value.

Trip setpoints 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, the associated device (e.g., digital trip module) changes state. The analytic limits are derived from the limiting values of the process parameters obtained from the safety analysis. [The Allowable Values are derived from the analytic limits, corrected for calibration, process and some of the instrument errors. The trip setpoints 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 channels that must function in harsh environments as defined by 10 CFR 50.49) are accounted for.

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 are required in each MODE to provide primary and diverse initiation signals.

NMS is required to be OPERABLE in MODE 6 with any control rod withdrawn from a core cell containing one or more fuel assemblies. Control rods withdrawn from a core cell containing no fuel assemblies do

BASES

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 NMS function is not required. In this condition the required SDM (LCO 3.1.1) and rod-out/rod pair interlock (LCO 3.9.2) ensure no event requiring RPS will occur. 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]) does not allow any control rod to be withdrawn. Under these conditions, the NMS 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.

<u>1.a, 1.b. Startup Range Neutron Monitor (SRNM) Neutron Flux—High, Neutron Flux—Short Period</u>

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 either an excessively high neutron flux level or for an excessive neutron flux increase rate, i.e., short reactor period. The setpoints of these trips are 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. 3). 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.

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 (upscale, or inoperative, or short period) will result in an SRNM division trip. Each SRNM divisional output is provided to each of the four divisions (SRNM interface unit). The SRNM interface 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. One channel from each bypass group may be bypassed from the operator's control console. 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.

Two SRNM Neutron Flux – High and two Neutron Flux - Short Period channels in three divisions 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 -High and Neutron Flux - Short Period Functions is set to mitigate the consequences of a rod withdrawal error.

The SRNM Neutron Flux - High Function must be OPERABLE during MODE 2 when control rods may be withdrawn and the potential for criticality exists. In MODE 6 when a cell with fuel has its control rod withdrawn the SRNMs provide monitoring for and protection against unexpected reactivity excursions. In MODE 1, the APRM System provide protection against control rod withdrawal error events and the SRNMs are not required.

<u>1.c. SRNM - Inop</u>

This trip signal provides assurance that a minimum number of SRNMs are OPERABLE. Anytime a SRNM detector voltage drops below a preset level, or when one of the modules is not plugged in, an inoperative trip signal will be received by the RPS 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.

Two SRNM – Inop channels in three divisions 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 - High and the Neutron Flux—Short Period Functions are required.

2.a. APRM 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 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 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 Neutron Flux—High, Setdown Function will provide the primary trip signal for a core wide increase in power.

No specific safety analyses take direct credit for the APRM Neutron Flux—High, Setdown, Function. 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.

The APRM system is divided into four divisions. Three channels of APRM 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, to provide adequate coverage of the entire core, at least [40] LPRM inputs are required to be OPERABLE.

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

The APRM Neutron Flux—High, Setdown Function must be OPERABLE during MODE 2 when control rods may be withdrawn and MODE 6 with any control rod withdrawn from a core cell containing one or more fuel assemblies since the potential for criticality exits. In MODE 1, the APRM Neutron Flux-High Function provides protection against reactivity transients.

BASES

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 neutron flux is electronically filtered with a time constant representative of the fuel heat transfer dynamics to generate a signal proportional to the thermal power in the reactor. The signal is fixed at an upper limit that is always lower than the APRM Fixed Neutron Flux—High Function Setpoint. The APRM Simulated Thermal Power - High Function provides protection against transients where thermal power increases slowly (such as the Loss of Feedwater Heating event) and protects the fuel clad integrity by ensuring the Minimum Critical Power Ratio (MCPR) Safety Limit is not exceeded. 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.

The APRM system is divided into four divisions. Three divisions 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 fixed Allowable Value for the APRM Simulated Thermal Power-High Function is intended for the mitigation of the Loss of Feedwater Heater event.

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 (MCPR Safety Limit). During MODES 2 and 6, other SRNM and APRM Functions provide protection for fuel cladding integrity.

2.c. APRM Fixed Neutron Flux - High

The APRM channels provide the primary indication of neutron flux within the core and respond almost instantaneously to neutron flux increases. The APRM Fixed Neutron Flux - High Function is capable of generating a trip signal to prevent fuel damage or excessive reactor coolant system pressure. For the overpressurization protection analysis of Reference 4, 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.

The APRM system is divided into four divisions. 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 is based on the Analytical Limit assumed in the turbine trip and generator load rejection analyses.

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 Limits (e.g., MCPR, and Reactor Vessel pressure) being exceeded. In MODE 2, the APRM 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.

<u>2.d. APRM - Inop</u>

This signal provides assurance that a minimum number of APRMs are OPERABLE. Anytime an APRM mode switch is moved to any position other than “Operate”, an APRM module is unplugged, the electronics operating voltage is low or the APRM has too few LPRM inputs (< [40]), an inoperative trip signal will be received by the RPS, 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

3. Oscillation Power Range Monitor

The Oscillation Power Range Monitor (OPRM) consists of four independent Class 1E channels. The OPRM channel utilizes the same set of LPRM signals used by the associated APRM channel in which this OPRM channel resides. Each OPRM receives the identical LPRM signals from the corresponding APRM channel as inputs, 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 algorithm detects thermal hydraulic instability (flux oscillation with unacceptable amplitude and frequency) and provides trip output to the RPS if the trip setpoint is exceeded. (The ESBWR OPRM trip protection algorithm will be determined in the COL phase.)

The OPRMs are divided into four divisions. 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, to provide adequate coverage of the entire core, at least [40] LPRM inputs are required to be OPERABLE.

The Allowable Value [later].

The OPRM Function is required to be OPERABLE in MODE 1 and 2 to respond to core neutron flux oscillation conditions and thermal-hydraulic instability in time to prevent safety thermal limit violation and fuel damage. In MODES 3, 4, 5, and 6, core neutron flux oscillation conditions and thermal-hydraulic instability is not postulated to occur and therefore the monitors are not required to be OPERABLE.

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 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

With one or more NMS Functions with one or more required instrumentation channels inoperable, the affected NMS division must be placed in trip. Because of the diversity of sensors available to provide trip signals and the redundancy of the NMS and RPS design, an allowable out of service time of [12] hours is considered acceptable to permit restoration of any inoperable channel to OPERABLE status. However, this out of service time is only acceptable provided the associated Function still maintains NMS trip capability (refer to Required Actions B.1 and C.1 Bases). If the inoperable channel cannot be restored to OPERABLE status within the allowable out of service time, the affected NMS division must be placed in trip. Placing the NMS division in trip would conservatively compensate for the inoperability and allow operation to continue. Alternately, if it is not desired to place the NMS division in trip (e.g., as in the case where placing the NMS division in trip would result in a full scram), Condition D must be entered and its Required Action taken. Most repairs are likely to be simple card or other electronic subassembly replacements that can be done on-line with the affected division of sensors in bypass. In such cases, restoration should be done as soon as practicable.

B.1

Condition B exists when, for any one or more SRNM Functions, at least one required channel inoperable in two or more required divisions. In this condition, provided at least one channel in two NMS SRNM divisions is OPERABLE or in trip, the SRNM Function still maintains trip capability for that Function, but cannot accommodate a single failure.

Required Actions B.1 limits the time the NMS SRNM Function, would not accommodate single failure. Within the 6 hour allowance, the associated Function will have one NMS division in trip.

Completing the Required Action restores NMS scram capability to a reliability level.

C.1

Required Action C.1 is intended to ensure that appropriate actions are taken 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 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 divisions to have one channel OPERABLE or in trip (or the associated APRM division in trip).

The Completion Time is intended to allow the operator time to evaluate and repair any discovered inoperabilities. The 1 hour Completion Time is acceptable because it minimizes risk while allowing time for restoration or tripping of channels.

D.1

Required Action D.1 directs entry into the appropriate Condition referenced in Table 3.3.1.4-1. 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. Each time an inoperable channel has not met any Required Action of Condition A, B, or C and the associated Completion Time has expired, Condition D will be entered for that channel and provides for transfer to the appropriate subsequent Condition.

E.1 and F.1

If a channel is not restored to OPERABLE status or placed in trip (or the associated division is placed in trip) within the allowed Completion Time, or if NMS trip capability is not restored with the allowed Completion Time, 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.

G.1

If a channel is not restored to OPERABLE status or placed in trip (or the associated division is placed in trip) within the allowed Completion Time, or if NMS trip capability is not restored with the allowed Completion Time, 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

The Surveillances are modified by a Note to indicate that a 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 or up to 6 hours provided the associated Function maintains trip capability. Upon completion of the Surveillance, or expiration of the 6 hour allowance, the channel must be returned to OPERABLE status or the applicable Condition entered and Required Actions taken. This Note is based on the assumption that 6 hours is the average time required to perform channel surveillance. The 6 hour testing allowance does not significantly reduce the probability that the RPS will trip when necessary.

<u>SR 3.3.1.4.1</u>

Performance of the CHANNEL CHECK once every 24 hours ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is a comparison of the parameter indicated on one channel to the same parameter on other channels. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value. Significant deviations between the instrument channels could be an indication of excessive instrument drift on one of the channels or even something more serious. 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 CHECK supplements less formal, but more frequent, checks of channel 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 APRM calibration based on heat balance results is calculated automatically by a process computer function. Manual initiation of the automatic APRM calibration update function is required to implement the new APRM gain factors. 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 3.3.1.4.4 (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 and APLHGR). At ≥ 25% RTP, the surveillance is required to have been satisfactorily performed within the last 7 days in accordance with SR 3.0.2.

SR 3.3.1.4.3

A CHANNEL FUNCTIONAL TEST is performed on each channel to ensure that the entire channel will perform the intended function when required.

If the as-found setpoint is not within its required Allowable Value the plant specific setpoint methodology may be revised, as appropriate, if the history and all other pertinent information indicates a need for the revision. The setpoint shall be left set consistent with the assumptions of the current plant-specific setpoint methodology.

As noted, for Functions 1.a, 1.b, 1.c, 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 7 day 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 92 days provides an acceptable level of system average unavailability over the Surveillance Frequency interval.

SR 3.3.1.4.4

LPRM gain settings are determined from the local flux profiles measured by the automated fixed incore probe (AFIP) subsystem of NMS. This establishes the relative local flux profile for appropriate representative input to the APRM system. The [1000] MWD/T Surveillance Frequency is based on operating experience with LPRM sensitivity changes.

SR 3.3.1.4.5

A 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 account for instrument drifts between successive calibrations. Measurement and setpoint error historical determinations must be performed consistent with the plant specific setpoint methodology. The channel shall be left calibrated consistent with the assumptions of the setpoint methodology.

If the as-found setpoint is not within its required Allowable Value the plant specific setpoint methodology may be revised, as appropriate, if the history and all other pertinent information indicates a need for the revision. The setpoint shall be left set consistent with the assumptions of the current plant-specific setpoint methodology.

SR 3.3.1.4.5 is modified by two Notes. Note 1 states, for Functions 1.a, 1.b, 1.c, 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 7-day 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 7-day calorimetric calibration (SR 3.3.1.4.2) and the [1000] MWD/T LPRM calibration (SR 3.3.1.4.4). The Surveillance Frequency of SR 3.3.1.4.5 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 3.3.1.4.6

The APRM Simulated THERMAL POWER - High Function uses an electronic filter circuit to generate a signal proportional to the core THERMAL POWER from the APRM neutron flux signal. This filter circuit is representative of the fuel heat transfer dynamics that produce the

BASES

relationship between the neutron flux and the core THERMAL POWER. The filter 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 3.3.1.4.7

The LOGIC SYSTEM FUNCTIONAL TEST demonstrates the OPERABILITY of the required trip logic for a specific channel. 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 Surveillance Frequency was developed considering it is prudent that the Surveillances be performed only during a plant outage. This is due to the plant conditions needed to perform the surveillance and the potential for unplanned transients if the surveillance is 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 3.3.1.4.8

This SR ensures that the individual channel response times are less than or equal to the maximum values assumed in the accident analysis.

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

RPS RESPONSE TIME tests are conducted on a 24 month STAGGERED TEST BASIS. Therefore, staggered testing results in response time verification of these devices every 24 months. The 24 month test Frequency is consistent with the typical industry refueling cycle and is based upon plant operating experience, which shows that random failures of instrumentation components causing serious time degradation, but not channel failure, are infrequent occurrences.

REFERENCES

1. Chapter 7, Figure 7.2-1.

2. Chapter 15.

BASES

3. Section 17.7.

4. Section 15.5.

B 3.3 INSTRUMENTATION

B 3.3.1.5 Nuclear Monitoring Instrument (NMS) Automatic 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.

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...so chosen that automatic protective action will correct the abnormal situation before a Safety Limit (SL) is exceeded." The Analytic Limit is the limit of the process variable at which a safety action is initiated, as established by the safety analysis, to ensure that a SL is not exceeded. Any automatic protection action that occurs on reaching the Analytic Limit therefore ensures that the SL is not exceeded. However, in practice, the actual settings for automatic protective devices must be chosen to be more conservative than the Analytic Limit to account for instrument loop uncertainties related to the setting at which the automatic protective action would actually occur.

The NMS is composed of the startup range neutron monitor (SRNM) and the average power range monitor (APRM). Separate, isolated, digital Startup Range Neutron Monitor (SRNM) trip signal and Average Power Range Monitor (APRM) trip signal 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 upscale (high count rate or high flux level); Short (fast) period; and SRNM inoperative. The three 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.

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 (upscale, or inoperative, or short period) will result in an SRNM division trip. Each SRNM divisional output is provided to each of the four divisions (SRNM interface unit). The SRNM interface 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. One channel from each bypass group may be bypassed from the operator's control console. 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.

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 high neutron flux, high simulated thermal power; and APRM inoperative.

There are four APRM channels divided into four NMS divisions. For each division, any one APRM channel trip (upscale or inoperative) will result in an division trip. Each APRM divisional output is provided to each of the four divisions (APRM interface unit). The SPRM interface unit determines whether there are sufficient SRNM divisions in trip (two-out-of-four logic). One APRM channel from may be bypassed at any one time.

The APRMs 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 and one for SRNM trip/no-trip. A divisional APRM 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 tripped or SRNM tripped basis, by looking at the four divisions of APRM and four divisions of SRNM. All bypasses of the SRNMs and APRMs are performed within and by the NMS.

BASES

This Specification covers the NMS automatic actuation channels that include the SRNM interface units, the APRM interface units and the associated output to RPS (LCO 3.3.1.1). LCO 3.3.1.4, covers SRNM and APRM channel inputs to the SRNM interface units..

APPLICABLE SAFETY ANALYSES

The actions of the NMS are assumed in the safety analyses of Reference 2. The NMS provides a trip signal to RPS which 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. NMS automatic actuation channels support the OPERABILITY of the RPS Instrumentation, “LCO 3.3.1.1, Reactor Protection System (RPS) Instrumentation” and therefore is required to be OPERABLE. This Specification covers the NMS actuation circuitry that covers the interface units and the associated output to RPS.

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

LCO

Three NMS SRNM automatic actuation channels and three NMS APRM automatic actuation channels are required to be OPERABLE to ensure no single automatic actuation channel failure will preclude a scram to occur on a valid signal. This Specification covers the NMS actuation circuitry that covers the interface units and the associated output to RPS.

APPLICABILITY

The NMS SRNM automatic actuation channels 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 RPS 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, NMS automatic actuation is not required to be OPERABE in these MODES.

The NMS APRM automatic actuation channels 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 NMS 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 OPERABE in these MODES. In MODE 6 with any control rod withdrawn from a core cell containing one or more fuel assemblies, the NMS 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 OPERABE in these MODES.

ACTIONS

A Note has been provided to modify the ACTIONS related to RPS automatic actuation 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 automatic actuation 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 automatic actuation channel.

A.1

Because of the redundancy of NMS automatic actuation channels available, an allowable out of service time of 12 hours is considered an acceptable to permit restoration of any required inoperable channel to OPERABLE status. However, this out of service time is only acceptable provided there is only one required inoperable NMS automatic actuation channel in the associated Function and the Function still maintains NMS trip capability (refer to Required Action B.1 Bases). If the inoperable channel cannot be restored to OPERABLE status within the allowable out of service time, the affected actuation division must be placed in trip. This is acceptable because the capability to accommodate a single failure exists and the reliability of the NMS automatic actuation logic. Placing the actuation division in trip would conservatively compensate for the inoperability, restore capability to accommodate a single failure, and allow operation to continue. Alternately, if it is not desired to place actuation division in trip (e.g., as in the case where placing the inoperable channel in trip would result in a full scram), Condition C must be entered and its Required Action taken.

B.1

Condition B exists when one or more Functions have two or more required NMS automatic actuation channels inoperable. Required Action B.1 is intended to ensure that appropriate actions are taken if multiple, inoperable, untripped channels (i.e., two or more required 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 channels 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 channels, two channels must be OPERABLE or in trip to maintain NMS trip capability.

The Completion Time is intended to allow the operator time to evaluate and repair any discovered inoperabilities. The 1 hour Completion Time is acceptable because it minimizes risk while allowing time for restoration or tripping of channels. Alternately, if it is not desired to place actuation division in trip (e.g., as in the case where placing the inoperable channel in trip would result in a full scram), Condition C must be entered and its Required Action taken.

C.1

Required Action C.1 directs entry into the appropriate Condition referenced in Table 3.3.1.5-1. 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. Each time an inoperable channel has not met any Required Action of Condition A or B, and the associated Completion Time has expired, Condition C will be entered for that channel and provides for transfer to the appropriate subsequent Condition.

D.1 and E.1

If the affected actuation division is not restored to OPERABLE status, the affected actuation division is not placed in trip, or if NMS automatic actuation capability is not restored, within the allowed Completion Time(s), 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

SURVEILLANCE REQUIREMENTS	The Surveillances are modified by a Note to indicate that a 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 or up to 6 hours provided the associated Function maintains trip capability. Upon completion of the Surveillance, or expiration of the 6 hour allowance, the channel must be returned to OPERABLE status or the applicable Condition entered and Required Actions taken. This Note is based on the assumption that 6 hours is the average time required to perform channel surveillance. The 6 hour testing allowance does not significantly reduce the probability that the NMS will trip when necessary. <u>SR 3.3.1.5.1</u> The LOGIC SYSTEM FUNCTIONAL TEST demonstrates the OPERABILITY of the NMS automatic actuation channels. 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.
REFERENCES	1. Chapter 7, Figure 7.2-1. 2. Chapter 15.

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 monitors for a total of twelve monitors. Each having one fixed in-core regenerative fission chamber sensor. They are connected to their designated preamplifiers located in the reactor building. The SRNM preamplifier signals are transmitted to the SRNM digital processing equipment units, which provide algorithms for signal processing and calculation to provide neutron flux, power calculations, period trip margin, period calculations, and provide various outputs for local and control console displays, recorder, and to the plant computer. The individual SRNM channel trips are combined to form a SRNM divisional trip in the NMS Divisional Interface Unit function. This SRNM divisional trip is sent to a SRNM interface unit function in each division that processes the SRNM trip signal of this division with trip inputs from all other three SRNM divisions to form a 2-out-of-4 voting logic. This final trip output from each of the four divisions is sent to the RPS. Alarm and trip outputs are also provided for both high flux and short period trip or alarm conditions. Such outputs also include the instrument inoperative trip. The electronics for the SRNMs and their designated bypass units are located in four separate cabinets, one in each of the four division locations. Each of the SRNM divisions can be bypassed, but only one at any given time, by the operation of a bypass switch. In addition, each individual monitor within each division may be bypassed. The SRNM instrumentation is discussed in detail in Ref. 1. 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 or special movable detectors connected to the normal SRNM circuits. 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.

BASES

APPLICABLE SAFETY ANALYSES	Prevention and mitigation of prompt reactivity excursions during refueling and low-power operation is provided by: LCO 3.9.1, “Refueling Equipment Interlocks,” 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, Nuclear Monitoring Instrumentation System (NMS) Instrumentation;" LCO 3.3.1.5, Nuclear Monitoring System (NMS) Actuation;" and LCO 3.3.2.1, “Control Rod Block Instrumentation.” 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 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 an adjacent quadrant. These requirements ensure that the reactivity of the core will be continuously monitored during CORE ALTERATIONS.

BASES

Special movable detectors according to Table 3.3.1.6-1, footnote (b), may be used during CORE ALTERATIONS in place of the normal SRNM nuclear detectors. These special detectors must be connected to the normal SRNM circuits in the NMS such that the applicable neutron flux indication can be generated. These special detectors provide more flexibility in monitoring reactivity changes during fuel loading, since they can be positioned anywhere within the core during refueling. They must still meet the location requirements of SR 3.3.1.6.2, and all other required SRs for SRNMs.

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.

ACTIONS

A.1 and A.2

With one or more required SRNM channels inoperable in MODE 3 or 4, 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 takes into account the low probability of an event requiring the SRNM occurring during this time.

B.1 and B.2

With one or more required SRNMs inoperable in MODE 5, 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.

BASES

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. A CHANNEL CHECK is a comparison of the parameter indicated on one channel to the same parameter indicated on other similar channels. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value. Significant deviations between the two instrument channels could be an indication of excessive instrument drift in one of the channels or even something more serious. A CHANNEL CHECK will detect gross channel failure; thus; it is key to verifying that the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

Agreement criteria are determined by the plant staff, based on a combination of the channel instrument uncertainties, including indication and readability. If a channel is outside the 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 and, 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.

BASES

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.

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. Verification of the signal-to-noise-ratio also ensures that the movable detectors, if used, are inserted to a normal operating level. In a fully withdrawn condition, these movable detectors are sufficiently removed from the fueled region of the core to essentially eliminate neutrons from reaching the detector. Any count rate obtained while fully withdrawn is assumed to be “noise” only. 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

BASES

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. SR 3.3.1.6.5 is required in MODE 6, and the 7 day Frequency is to ensure that the channels are OPERABLE while core reactivity changes could be in progress. This 7 day Frequency is reasonable, based on operating experience and other Surveillances, such as a CHANNEL CHECK, that provide assurance of proper functioning between CHANNEL FUNCTIONAL TESTS.

SR 3.3.1.6.6 is required in MODES 3, 4, and 5. Since core reactivity changes do not normally take place, the Frequency has been extended from 7 days to 31 days. 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 Frequency considers the unit conditions required to perform the test, the ease of performing the test, and a 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 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

1. Section 7.2.

B 3.3 INSTRUMENTATION

B 3.3.1.7 Standby Liquid Control (SLC) and Feedwater Runback (FWRB) Instrumentation

BASES

BACKGROUND

The safety-related portions of the Anticipated Transient Without Scram (ATWS) mitigation logic, which provide an alternate means of reactivity reduction to protect against the remote probability of a failure to insert all control rods when needed, are contained within the four divisions of the Safety System Logic and Control (SSLC), but as part of circuitry that is separate and diverse from the software-based Reactor Protection System (RPS) logic as described in Sections 7.2.1 and 7.8.1.1 (Refs. 1 and 2).

The SSLC is comprised of four independent logic divisions (Division I, II, III, and IV). For the RPS logic, each logic division provides protective action initiation signals for safety system prime movers associated with their division. Each division is a collection of SENSOR CHANNELS, which provide data to the LOGIC CHANNELS in the division. The LOGIC CHANNELS provide initiation signals to the appropriate OUTPUT CHANNELS. The OUTPUT CHANNELS cause actuation of the equipment that implements protective actions.

For the safety-related ATWS mitigation logic, analog trip modules (ATMs), instead of the Digital Trip Modules (DTMs) used for the RPS logic, perform setpoint comparisons for the automatic trip parameters in each division for the ATWS SENSOR CHANNELS. A description of the ATWS LOGIC CHANNELS and ATWS OUTPUT CHANNELS, as well as the SLC and FWRB automatic actions, is contained in the Background section of the LCO 3.3.1.8, “Standby Liquid Control (SLC) and Feedwater Runback (FWRB) Actuation,” Bases.

Automatic initiation of SLC is from 1) reactor vessel steam dome pressure - high and a Startup Range Neutron Monitors (SRNMs) ATWS SLC permissive (i.e., SRNM signals above a specified setpoint for 3 minutes or greater), or 2) reactor vessel water level – low, level 2, and a SRNM ATWS SLC permissive for 3 minutes or greater.

Automatic initiation of FWRB is from reactor vessel steam dome pressure - high and a Startup Range Neutron Monitors (SRNMs) ATWS FWRB permissive (i.e., SRNM signals above a specified setpoint for 2 minutes or greater). Reset of FWRB is permitted only when both signals drop below the associated setpoints.

BASES

In the Diverse Protection System (DPS), a manual ATWS initiation signal to SSLC initiates boron injection from the SLC system and initiates Feedwater Control (FWC) runback of feedwater flow.

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

The safety-related features of the ATWS mitigation logic for SLC and FWRB are assumed in the analysis described in Reference 3. These features are initiated to aid in preserving the integrity of the fuel cladding following events in which a required scram may not occur. SLC and FWRB instrumentation are Functions not specifically credited in the accident analysis, but are retained for the overall redundancy and diversity of the RPS as required by the NRC approved licensing basis.

The OPERABILITY of SLC and FWRB is dependent on the OPERABILITY of the individual Functions. Each Function must have a required number of OPERABLE channels.

The individual Functions are required to be OPERABLE in MODES 1 and 2 to protect against postulated common mode failures of the RPS by providing a diverse method of reducing core reactivity. In MODES 1 and 2 the reactor may be producing significant power. In MODES 3, 4, and 5, the reactor is shut down with all control rods inserted; thus, an ATWS event is not credible. In MODE 6, the one-rod-out interlock ensures the reactor remains subcritical; thus, an ATWS event is not significant.

The LOGIC CHANNELS and OUTPUT CHANNELS are addressed in LCO 3.3.1.8. This LCO addresses the SENSOR CHANNELS. The discussions are given below on a Function-by-Function basis.

<u>1 and 2. Source Range Neutron Monitors – ATWS SLC and FWRB Permissive</u>

During some low power plant conditions the ATWS trips could interfere with normal plant maneuvering and cause unnecessary stress on plant equipment. In order to prevent the risks associated with the stresses, and to confirm that an ATWS may have occurred, the SLC and FWRB ATWS Functions are disabled at low Source Range Neutron Monitor (SRNM) neutron flux levels. The SRNM ATWS Permissive Function is used in the SLC and FWRB ATWS mitigation Features to permit initiation when the power level as detected by the SRNM is greater than the Allowable Value. When all of the unbypassed SRNM channels indicate that power level is less than the Allowable Value then the permissive is removed and the affected ATWS mitigation Features are automatically inhibited. This Function is implicitly assumed in the analysis of Section [15.] (Ref. 3).

This Function is required to be OPERABLE in MODES 1 and 2 since these are the MODES where the ATWS Functions must be OPERABLE. See LCO 3.3.1.8 Bases for the applicability basis.

The Allowable Value is selected high enough to permit the necessary plant maneuvers, and low enough to assure that ATWS is available when the plant power level will not permit long term cooling by the ECCS and their support systems. The associated time delay is provided to ensure a valid failure to scram the reactor has occurred requiring SLC and FWRB initiation.

3. 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 Reactor Coolant Pressure Boundary (RCPB). None of the safety analyses in Chapter 15 take direct credit for this Function. However, the RPS 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. Initiation of SLC and FWRB provide a diverse method to shutdown the reactor if a valid failure to scram the reactor occurs for these transients that result in a pressure increase.

Each ATM receives an analog signal directly from the process sensors for this Function. The ATM compares the signal with a setpoint to generate the ATWS SLC and FWRB initiation signal. Reactor pressure is measured using four independent (separate vessel taps, instrument piping, etc.) pressure transmitters connected to the RPV steam space. The four sensors are connected to both the Remote Multiplexing Unit (RMU) for SSLC Functions and ATM for SLC and FWRB Functions in the same division. The Reactor Vessel Steam Dome Pressure - High Allowable Value is chosen to provide a sufficient margin to the ASME Section III Code limits during pressurization events.

Four divisions of Reactor Vessel Steam Dome Pressure - High Function are required to be OPERABLE to ensure that no single instrument failure will preclude a protective action from this Function on a valid signal. This Function is required to be OPERABLE in MODES 1 and 2 since these are

BASES

the MODES where the ATWS Functions must be OPERABLE. See LCO 3.3.1.8 Bases for the applicability basis.

4. Reactor Vessel Water Level – Low, Level 2

Should RPV water level decrease too far, fuel damage could result. Reactor Vessel Water Level – Low, Level 2 indicates that normal feedwater flow is insufficient to maintain reactor vessel water level and that the capability to cool the fuel may be threatened. Therefore, various actions are initiated at Level 2 to assist in maintaining water level above the active fuel. Prior to reaching Level 2 on decreasing RPV water level, a Reactor Vessel Water Level – Low, Level 3 signal initiates a reactor scram to reduce core power. Initiation of SLC and FWRB provide a diverse method to shutdown the reactor if a valid failure to scram the reactor occurs for these transients that result in a Level 2 condition.

Each ATM receives an analog signal directly from the process sensors for this Function. The ATM compares the signal with a setpoint to generate the ATWS SLC and FWRB initiation signal. The reactor water level signals originate in four independent (separate vessel taps, instrument piping, etc.) level transmitters that sense the pressure difference between a constant column of water (reference leg) and the effective water column (variable leg) in the vessel. The four sensors are connected to both the RMU for SSLC Functions and ATM for SLC and FWRB Functions in the same division. The Reactor Vessel Water Level – Level 2 Allowable Value is chosen to detect a complete loss of feedwater flow at a RPV water level sufficient to ensure that the active fuel remains covered for all analyzed events.

Four divisions of Reactor Vessel Water Level - Low, Level 2 Function are required to be OPERABLE to ensure that no single instrument failure will preclude a protective action from this Function on a valid signal. This Function is required to be OPERABLE in MODES 1 and 2 since these are the MODES where the ATWS Functions must be OPERABLE. See LCO 3.3.1.8 Bases for the applicability basis.

ACTIONS

A Note has been provided to modify the ACTIONS related to SLC and FWRB 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 SLC and FWRB 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 SLC and FWRB Instrumentation channel.

<u>A.1, A.2.1.1, A.2.1.2, A.2.2.1, and A.2.2.2</u>

A SENSOR CHANNEL is considered to be OPERABLE when all components or devices required to provide the results of a trip calculation to the LOGIC CHANNELS that use the data from the channel are OPERABLE. If any LOGIC CHANNEL that uses the trip data from a SENSOR CHANNEL does not receive valid data then the channel is considered to be inoperable.

Since each Function has four SENSOR CHANNELS, a failure in one SENSOR CHANNEL will cause the initiation logic to become 1/3 or 2/3 depending on the nature of the failure (i.e., failure which causes a channel trip vs. a failure which does not cause a channel trip). Therefore, an additional single failure will not result in loss of protection but could cause a spurious initiation of a protective action for additional failures that result in a tripped condition.

Action A.1 forces a trip condition in the inoperable SENSOR CHANNEL, which causes the initiation logic to become 1/3 for the specific Functions that are placed in trip. In this condition a single failure will not result in loss of protection. This Action is applicable when more than one Function has a single inoperable SENSOR CHANNEL without regard to the divisions containing the failed channels. In this condition, the availability of the Function to provide a plant protective action is at least equivalent to the 2/4 trip logic. Since plant protection capability is within the design basis no further action is required when the inoperable SENSOR CHANNEL is placed in trip.

Action A.2.1.1 bypasses all SENSOR CHANNELS, except the Neutron Monitoring System (NMS), in the division containing the inoperable SENSOR CHANNEL. This causes the logic for affected Functions in all four divisions to become 2/3 so a single failure will not result in loss of protection or cause a spurious initiation. However, the degree of redundancy is reduced. As indicated by a note in the LCO, this action is not applicable to the NMS Functions. This action may be implemented for single SENSOR CHANNEL failures in multiple Functions only when all failures are in the same division.

BASES

Action A.2.1.2 is similar to Action A.2.1.1 but applies only to the NMS Functions as indicated by a note in the LCO. The NMS trip logic in all NMS divisions then becomes 2/3 and remains as 2/4 in the SLC and FWRB Instrumentation Functions. In this condition a single failure will not result in loss of protection or cause a spurious initiation.

The SRNM is bypassed or tripped by tripping or bypassing the individual SENSOR CHANNELS. Bypass must be accomplished using the three SRNM bypass switches as described in LCO 3.3.1.4, "Neutron Monitoring System (NMS) Instrumentation," Bases. This arrangement also prevents bypassing all Division II sensors; therefore, failure of all Division II sensors requires taking the trip action. For the SRNM, any inoperable SENSOR CHANNEL must be bypassed even if the associated SSLC SRNM division remains OPERABLE. The requirement for the individual SRNM channel bypass is controlled by LCO 3.3.1.4

The Completion Time of twelve hours for implementing Actions A.1, A.2.1.1, and A.2.1.2 is based on providing sufficient time for the operator to determine which of the actions is appropriate. The Completion Time is acceptable because the probability of an event requiring the Function coupled with a failure in another SENSOR CHANNEL of the same Function occurring within that time period is low.

Action A.2.2.1 restores all required SENSOR CHANNELS for the Function to the OPERABLE status following completion of Action A.2.1.1 or A.2.1.2. Action A.2.2.2 provides an alternate to A.2.2.1. Both of these Actions place the SLC and FWRB within the SLC and FWRB availability design basis.

Implementing Actions A.2.1.1 or A.2.1.2 provides confidence that the diverse plant protection provided by SLC and FWRB is maintained given an additional single failure, and the self-test features of the NMS and the required Surveillances for SLC and FWRB Instrumentation will detect most failures, so operation in this condition for 30 days is acceptable. Also, the Probabilistic Risk Assessment (PRA) analysis has shown that the change in core damage frequency is negligible with three instead of four OPERABLE divisions of sensors.

Note 1 for Action A.2.2.2 requires that the bypass implemented per Action A.2.1.1 or A.2.1.2 be removed after implementing Action A.2.2.2. This is necessary to restore the SLC and FWRB to within its availability design basis. Note 2 is included to permit a division of sensors or NMS division bypass for a limited period to permit repairs. Note 3 is included to permit placing a division in division of sensors bypass even if the division contains SENSOR CHANNELS that were tripped due to previous entries into the condition. Placing a division in division of sensor bypass masks any SENSOR CHANNEL manual trips in the division. This configuration is acceptable for the period of time that a division of sensor bypass is permitted under other actions of Condition A.

B.1, B.2.1.1, B.2.1.2, and B.3

Condition B occurs when two SENSOR CHANNELS for the same Function become inoperable. In this condition the initiation logic could be 2/2 so a single failure would cause loss of initiation from the Function.

Placing one of the failed SENSOR CHANNELS in trip (Action B.1) causes the trip logic to become 1/2 so a failure in an additional SENSOR CHANNEL for the function will not prevent initiation of a protective action from the Function. The six-hour Completion time for this Action provides sufficient time for the operator to implement the Action. Operation for this amount of time does not contribute significantly to plant risk because the probability of an event requiring the Function, coupled with an undetected Failure in one of the remaining channels for the Function, within the time period is quite low.

Action B.2.1.1 requires placing the division containing the second failed SENSOR CHANNEL in division of sensors bypass for those Functions given in the LCO note. Action B.2.1.2 requires a similar action for inoperable NMS channels. Performing these actions will prevent a change in status of the inoperable channel from causing a spurious initiation of a protective action. A Completion Time of 12 hours is permitted for these actions. The probability of the failed channel causing a spurious initiation during this time period is quite low.

Action B.3 restores at least one of the failed channels to OPERABLE status. A Completion Time of 30 days is permitted for this Action. The Completion Time is based on the low probability of an undetected failure in both of the OPERABLE channels for the Function occurring in that time period. The self-test features of the NMS, and the required Surveillances for SLC and FWRB Instrumentation, provide a high degree of confidence that no undetected failures will occur in the allowable Completion Time.

C.1 and C.2

This Condition applies when three SENSOR CHANNELS for the same Function become inoperable. This Condition represents a case where automatic protective action from a Function is 1/1 (one of the channels fails in a tripped state) or is completely unavailable.

Action C.1 causes the initiation logic to become 1/1 so a protective Action from the Function is still available but the single failure criteria for automatic actuation is not met. However, other diverse trip parameters are available, including manual initiation.

Action C.2 causes restoration of a second channel for the Function so the initiation logic becomes 1/2 and plant protection is maintained for a single additional failure. The six-hour Completion Time for Action C.2 provides a reasonable amount of time to effect repairs on at least one of the inoperable channels and avoid the risks associated with plant shutdown.

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

This Condition applies when all of the SENSOR CHANNELS for the same Function become inoperable. This Condition represents a case where automatic protective action from a Function is completely unavailable. However, other diverse trip parameters are available, including manual initiation.

Although Action D.1 does not restore the initiation capability from the Function it is required so that the logic will become 1/1 when Action D.2 is completed.

Action D.2 causes restoration of at least one channel for the Function, which causes the initiation logic to become 1/1 so protective action for the Function is restored. The one-hour Completion Time for Action D.2 provides some amount of time to effect repairs on at least one of the inoperable channels and avoid the risks associated with plant shutdown. Plant operation in this condition for the specified time does not contribute significantly to plant risk because the probability of an event requiring the Function within the Completion Time is low.

<u>E.1</u>

Required Action E.1 directs entry into the appropriate Condition referenced in Table 3.3.1.7-1 if the Required Action and associated Completion Times of Conditions A, B, C, or D are not met. 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. Each time the entry condition is met, Condition E will be entered for that channel/division and provides for transfer to the appropriate subsequent Condition.

BASES

F.1

If the Required Actions for Conditions A, B, C, or D are not met within the specified Completion Times, the unit must be placed in a MODE that minimizes risk. To achieve this status, the unit must be placed in MODE 2 within 6 hours or remain in MODE 3. The allowable Completion Time is reasonable, based on operating experience, to reach the required unit conditions from full power conditions in an orderly manner and without challenging unit systems.

G.1

If the Required Actions for Conditions A, B, C, or D are not met within the specified Completion Times, the unit must be placed in a MODE or other specified condition in which the LCO does not apply. The allowable Completion Time is reasonable, based on operating experience, to reach the required unit conditions from full power conditions in an orderly manner and without challenging unit systems.

SURVEILLANCE REQUIREMENTS

As noted at the beginning of the SRs, the SRs for each SLC and FWRB Instrumentation Function are located in the SRs column of Table 3.3.1.7-1.

The Surveillances are modified by a Note to indicate that a 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 or up to 6 hours provided the associated Function maintains SLC and FWRB functional capability. Upon completion of the Surveillance, or expiration of the 6-hour allowance, the channel must be returned to OPERABLE status or the applicable Condition entered and Required Actions taken. This Note is based on the assumption that 6 hours is the average time required to perform channel Surveillance.

SR 3.3.1.7.1

Performance of the SENSOR CHANNEL CHECK once every 24 hours provides confidence that a gross failure of a device in a SENSOR CHANNEL has not occurred. A SENSOR CHANNEL CHECK is a comparison of the parameter indicated in one SENSOR CHANNEL to a similar parameter in a different SENSOR CHANNEL. It is based on the assumption that SENSOR CHANNELs monitoring the same parameter should read approximately the same value. Significant deviations between the channels could be an indication of excessive instrument drift on one of the channels or other channel faults. A SENSOR CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying the instrumentation continues to operate properly between each DIVISIONAL FUNCTIONAL TEST.

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 high reliability of each channel provides confidence that a channel failure will be rare. The SENSOR CHANNEL CHECK supplements less formal, but more frequent, checks of channel during normal operational use of the displays associated with the channels required by the LCO.

SR 3.3.1.7.2

A DIVISIONAL FUNCTIONAL TEST is performed on the SRNM channels in each division to provide confidence that the function will perform as intended.

If the as found trip point is not within its required Allowable Value, the plant specific setpoint methodology may be revised, as appropriate, if the history and all other pertinent information indicate a need for the revision. The as-left setpoint shall be consistent with the assumptions of the current plant specific setpoint methodology.

The devices that are used to implement the SRNM ATWS SLC and ATWS FWRB Permissive Functions are specified to be highly reliable and low drift. The self-test features provide confidence that most failures will be automatically detected. Therefore, a Frequency of 92 days is reasonable based on engineering judgment.

SR 3.3.1.7.3

A CHANNEL FUNCTIONAL TEST is performed on the required Functions or channels in each division to provide confidence that the Functions will perform as intended. The test is performed by replacing the process signal with a test signal as far upstream in the instrument channel as possible within the constraints of the instrumentation design and the need to perform the Surveillance without disrupting plant operations. The testing may be performed so that multiple uses of a parameter may be tested at one time.

If the as found trip point is not within its required Allowable Value, the plant specific setpoint methodology may be revised, as appropriate, if the history and all other pertinent information indicate a need for the revision. The setpoint shall be left set consistent with the assumptions of the current plant specific setpoint methodology.

The 92-day Frequency is the specified high reliability and low drift of the devices that are used to implement the Functions. The diversity of Functions provided for plant protection (including manual actuation), coupled with the SENSOR CHANNEL CHECKS, provide confidence that this Frequency is adequate.

The OPERABILITY of the SENSOR CHANNELs is determined by injecting a test signal in a single channel as near to the source as possible to assure that the ATMs in all divisions create an initiation signal when needed and that the signal is received by the LOGIC CHANNELS.

SR 3.3.1.7.4

The tests in the COMPREHENSIVE FUNCTIONAL TEST (CoFT) verify proper SLC and FWRB system function, computer component function, software and hardware interactions, response times, and error handling. Error statistics, usage statistics, historical statistics, and various other measures are used to verify proper performance of the SLC and FWRB. Successful completion of these tests establishes OPERABILITY of SENSOR CHANNELS, LOGIC CHANNELS, and OUTPUT CHANNELS.

The ESBWR protective action equipment is divided into segments to simplify software and hardware design and to limit the scope of effect of a given failure. A periodic test is performed to provide confidence that the segments and associated interconnections are operating within specified limits. The CoFT is designed to confirm that the current configuration and state of the system is acceptable and to determine the real-time performance of the overall system. Appropriately designed tests that include suitable data logging and analysis may be used to detect unexpected degradation.

The software-based SSLC system, and the diverse system for SLC and FWRB within the DPS, contain many states, not all of which will occur over the life of the plant. The most important states are those that are required to mitigate accidents. Therefore, the CoFT for both SSLC and DPS Functions focuses on usage testing, which exercises the overall system by simulating the input conditions under which the system is designed to perform, rather than coverage testing, which attempts to exercise all possible states of the system. Before plant start-up, there is a high level of confidence that the SSLC and DPS will operate as specified due to the extensive inspections, tests, and analyses conducted during the preoperational phases. During the plant operating life, the CoFT assures that the protective action equipment is within its specified performance characteristics.

The COMPREHENSIVE FUNCTIONAL TEST is intended to provide end-to-end testing. If necessary, other Surveillances (e.g., CHANNEL CALIBRATION, CHANNEL FUNCTIONAL TEST, etc.) that overlap the CoFT may be used to satisfy the requirements of the COMPREHENSIVE FUNCTIONAL TEST.

This Surveillance overlaps or is performed in conjunction with the output channel COMPREHENSIVE FUNCTIONAL TESTS in the LCOs that address the output channels and LCOs that test the final actuation devices. The combined or overlapping tests provide complete end-to-end testing of all protective actions associated with the SSLC and DPS for SLC and FWRB.

The 24 month Frequency is based on the ESBWR expected refueling interval, and the need to perform this Surveillance under the conditions that apply during a plant outage to reduce the potential for an unplanned transient if the Surveillance were performed with the reactor at power. The high reliability of the devices used in the SSLC and DPS processing coupled with the CHANNEL FUNCTIONAL TESTS and DIVISIONAL FUNCTIONAL TESTS provide confidence that the specified Frequency is adequate.

<u>SR 3.3.1.7.5</u>

A CHANNEL CALIBRATION is a complete check of the instrument loop and the sensor. This test verifies that a channel responds to the measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drifts between successive calibrations. Measurement and setpoint error historical determinations must be performed consistent with the plant specific setpoint methodology. The channel shall be left calibrated consistent with the assumptions of the setpoint methodology.

CHANNEL CALIBRATION includes calibration of the ATMs for SLC and FWRB. If the as-found setpoint is not within its required Allowable Value the plant specific setpoint methodology may be revised, as appropriate, if the history and all other pertinent information indicates a need for the revision. The setpoint shall be left set consistent with the assumptions of the current plant-specific setpoint methodology.

BASES

As noted, neutron detectors are excluded from CHANNEL CALIBRATION because of the difficulty of simulating a meaningful signal. Performing periodic CHANNEL CHECKs ensure that changes in SRNM neutron detector sensitivity are identified.

The 24-month Frequency is based on the ESBWR expected refueling interval and the need to perform this Surveillance under the conditions that apply during a plant outage. The Frequency is supported by a setpoint analysis that includes a drift allowance commensurate with this Frequency.

REFERENCES

1. Section 7.2.1.
2. Section 7.8.1.1.
3. Chapter 15.

B 3.3 INSTRUMENTATION

B 3.3.1.8 Standby Liquid Control (SLC) and Feedwater Runback (FWRB) Actuation

BASES

BACKGROUND

The safety-related portions of the Anticipated Transient Without Scram (ATWS) mitigation logic, which provide an alternate means of reactivity reduction to protect against the remote probability of a failure to insert all control rods when needed, are contained within the four divisions of the Safety System Logic and Control (SSLC), but as part of circuitry that is separate and diverse from the software-based Reactor Protection System (RPS) logic as described in Section 7.2.1 (Ref. 1).

The SSLC is comprised of four independent logic divisions (Division I, II, III, and IV). For the RPS logic, each logic division provides protective action initiation signals for safety system prime movers associated with their division. Each division is a collection of SENSOR CHANNELS, which provide data to the LOGIC CHANNELS in the division. The LOGIC CHANNELS provide initiation signals to the appropriate OUTPUT CHANNELS. The OUTPUT CHANNELS cause actuation of the equipment that implements protective actions.

A description of the ATWS SENSOR CHANNELS is contained in the Background section of the LCO 3.3.1.7, “Standby Liquid Control (SLC) and Feedwater Runback (FWRB) Instrumentation,” Bases. For the safety-related ATWS mitigation logic, hardware-based discrete digital logic, using a discrete-logic (non-microprocessor based) ATWS Logic Processor in each of the four SSLC cabinets as shown in Chapter 7, Figure 7.8-3 (Ref. 2), substitutes for the RPS software-based trip logic as part of the ATWS LOGIC CHANNELS. The ATWS Logic Processor performs the 2-out-of-4 voting function and additional interlock logic on data from analog trip modules (ATMs) and the Nuclear Monitoring System (NMS), and provides contact closure outputs hardwired to SLC and FWRB ATWS OUTPUT LOGIC.

The initiation signals from the four ATWS LOGIC CHANNELS are connected to a series/parallel arrangement of load drivers in the driven systems such that an initiation signal from any two of the ATWS LOGIC CHANNELS will cause actuation of SLC and FWRB ATWS mitigation features as part of the ATWS OUTPUT CHANNELS. The actuating signals for SLC and FWRB are hardwired (not multiplexed) to their respective system controllers. If one of the four ATWS Logic Processors is inoperable, bypass signals are sent to the SLC system and Feedwater Control (FWC) to bypass the input signals from the out-of-service

BASES

processor so that the input voting logic changes from 2-out-of-4 to 2-out-of-3. A manual bypass switch for this function is part of the SSLC Bypass Unit in each division. The bypass signals are isolated when connected to the nonsafety-related FWC and are interlocked so that multiple divisions cannot be bypassed simultaneously.

SLC injects a solution of Boron (a neutron absorber) and water into the reactor vessel. The available quantity of borated water is sufficient to reduce core reactivity to an acceptable level for a postulated failure of all control rods to be inserted. There are two SLC nitrogen-pressurized accumulators and associated explosive squib-actuated injection valves.

FWRB causes the feedwater pumps to go to minimum speed, which reduces core inlet subcooling and therefore core reactivity and power level. A runback signal is sent to each of the feedwater pumps.

In the Diverse Protection System (DPS), a manual ATWS initiation signal to SSLC initiates boron injection from the SLC system and initiates FWC runback of feedwater flow.

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

The safety-related features of the ATWS mitigation logic for SLC and FWRB are assumed in the analysis described in Reference 3. These features are initiated to aid in preserving the integrity of the fuel cladding following events in which a required scram may not occur. SLC and FWRB actuation are Functions not specifically credited in the accident analysis, but are retained for the overall redundancy and diversity of the RPS as required by the NRC approved licensing basis.

The OPERABILITY of SLC and FWRB is dependent on the OPERABILITY of the individual Functions. Each Function must have a required number of OPERABLE channels.

The individual Functions are required to be OPERABLE in MODES 1 and 2 to protect against postulated common mode failures of the RPS by providing a diverse method of reducing core reactivity. In MODES 1 and 2 the reactor may be producing significant power. In MODES 3, 4, and 5, the reactor is shut down with all control rods inserted; thus, an ATWS event is not credible. In MODE 6, the one-rod-out interlock ensures the reactor remains subcritical; thus, an ATWS event is not significant.

BASES

The SENSOR CHANNELS are addressed in LCO 3.3.1.7. This LCO addresses the LOGIC CHANNELS and OUTPUT CHANNELS. The discussions are given below on a Function-by-Function basis.

1.a, 2.a SLC and FWRB Actuation LOGIC CHANNELS

These LOGIC CHANNELS must generate and transmit initiation data to the OUTPUT CHANNELS. Each of the four channels sends initiation data to all four OUTPUT CHANNELS. Four channels of this Function are required to be OPERABLE and three are necessary to provide confidence that no single instrument failure can preclude SLC and FWRB initiation from this Function on a valid signal.

There is no allowable value associated with this Function.

1.b, 2.b SLC and FWRB Actuation OUTPUT CHANNELS

These OUTPUT CHANNELS cause actuation of SLC and FWRB. Protective action will occur when actuation signals occur in 2 of the 4 channels. Four channels are required to be OPERABLE and three channels must be OPERABLE to provide confidence that no single instrument failure can preclude a SLC and FWRB initiation from this Function on a valid signal.

3. Manual ATWS - ARI/SLC/FWRB Actuation

The Manual ATWS - ARI/SLC/FWRB Actuation pushbutton channels introduce signals into the SLC and FWRB logic to provide manual initiation capability that is redundant to the automatic initiation. There are two pushbuttons and both must be activated to initiate SLC and FWRB. Each switch has four contacts for SLC and FWRB actuation. Signals from both manual switches are sent to the logic in all four divisions. Each contact is a separate channel so there are two manual actuation-channels per division.

There is no Allowable Value for this Function since it is mechanically actuated based solely on the position of the pushbuttons. Two channels per division of the Manual Initiation Function are required to be OPERABLE when SLC and FWRB are required to be OPERABLE.

BASES

ACTIONS

A Note has been provided to modify the ACTIONS related to SLC and FWRB Actuation 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 SLC and FWRB Actuation channels provide appropriate compensatory measures for separate inoperable channels. As such, a Note has been provided which allows separate Condition entry for each inoperable SLC and FWRB Actuation channel.

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

These Actions assure that appropriate compensatory measures are taken when a LOGIC CHANNEL or manual initiation channel becomes inoperable in one division. A failure in one division will cause the logic to become 1/3 or 2/3 depending on the nature of the failure (i.e., failure which causes a trip vs. a failure which does not cause a trip). Therefore, an additional single failure will not result in loss of protection.

Action A.1 bypasses the inoperable channel, which forces the logic to become 2/3 so a single failure will not result in loss of protection or cause a spurious initiation. The Completion Time of twelve hours for implementing this Action provides sufficient time to perform the Action. Implementing Required Action A.1 provides confidence that plant protection is maintained for an additional single instrument failure.

Action A.2 requires the restoration of the inoperable channel within 30 days. This 30 day Completion Time is acceptable since completion of Action A.1 causes the logic to become 2/3.

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

These Actions assure that appropriate compensatory measures are taken when a LOGIC CHANNEL or manual initiation channel is inoperable in two divisions due to failures that do not cause an initiation. For this condition, the actuation logic becomes 2/2 or 1/2, depending on the nature of the failures.

Action B.1 bypasses one of the divisions containing the failed channel to permit repairs on that channel. Action B.2 restores at least one inoperable channel to OPERABLE status.

BASES

The Completion Time of 12 hours for implementing Action B.1 is based on providing sufficient time for the operator to determine which of the failed channels to bypass and to perform the Action. The Completion Time is acceptable because the probability of an event requiring the Function, coupled with a failure that would defeat the other channels associated with the Function, occurring within that time period is low.

When Action B.1 is completed, protective action is maintained as long as the other channels remain OPERABLE.

Therefore, operation in this condition is permitted for 7 days (Action B.2 Completion Time). The probability of an event requiring plant scram, combined with failure to scram and an undetected failure in another channel of the Function, within the Completion Time is quite low.

C.1

This Action assures that appropriate compensatory measures are taken when one OUTPUT CHANNEL of a Function becomes inoperable. For these Functions, a failure in one OUTPUT CHANNEL will cause the actuation logic to become 1/3 or 2/3 depending on the nature of the failure (i.e., failure which causes a channel trip vs. a failure which does not cause a channel trip). Therefore, an additional single failure will not result in loss of protection.

Action C.1 restores the channel to OPERABLE status. Since plant protection action is maintained given an additional single failure, operation in this condition for 30 days is permitted. The Completion Time is acceptable because the probability of an event requiring plant scram, combined with failure to scram and undetected failures that would defeat two other channels associated with the Function, occurring within that time period is quite low.

D.1

These actions are intended to ensure that appropriate actions are taken when two OUTPUT CHANNELS become inoperable. For this Condition the actuating logic becomes 2/2 so automatic initiation capability is maintained.

The Completion Time to restore one of the inoperable channels is sufficient for the operator to take corrective action and takes into account the low likelihood of an event requiring actuation of the SLC and FWRB coupled with a failure in an additional channel during this period.

BASES

E.1

With any Required Action and associated Completion Time not met, or multiple failures that cause the loss of a Function or the logic to become 1/1 the SLC must be declared inoperable. This will cause the LCO for an inoperable SLC to be invoked and appropriate compensatory measures taken.

The allowed Completion Time provides sufficient time to perform the Actions.

SURVEILLANCE REQUIREMENTS

As noted at the beginning of the SRs, the SRs for each SLC and FWRB Actuation Function are located in the SRs column of Table 3.3.1.18-1.

The Surveillances are modified by a Note to indicate that a 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 or up to 6 hours provided the associated Function maintains SLC and FWRB functional capability. Upon completion of the Surveillance, or expiration of the 6-hour allowance, the channel must be returned to OPERABLE status or the applicable Condition entered and Required Actions taken. This Note is based on the assumption that 6 hours is the average time required to perform channel Surveillance.

SR 3.3.1.8.1

A DIVISIONAL FUNCTIONAL TEST is performed on each required LOGIC CHANNEL and manual channel to ensure that the Functions will perform as intended. The test is performed by replacing the normal signal with a test signal as far upstream in the channel as possible within the constraints of the instrumentation design and the need to perform the Surveillance without disrupting plant operations. See Specification 1.1, “Definitions,” for additional information on the scope of the test.

The devices used to implement the SLC and FWRB Actuation Functions are specified to be highly reliable and have a high degree of redundancy. Therefore, the 92-day Frequency provides confidence that device actuation will occur when needed. This test overlaps or is performed in conjunction with the DIVISIONAL FUNCTIONAL TESTS performed under LCO 3.3.1.7, “Standby Liquid Control (SLC) and Feedwater Runback (FWRB) Instrumentation,” to provide testing up to the OUTPUT CHANNEL.

BASES

The devices used to implement the SLC and FWRB Actuation Functions are specified to be of high reliability and have a high degree of redundancy. Therefore, the 92-day Frequency provides confidence that device actuation will occur when needed.

SR 3.3.1.8.2

The LOGIC SYSTEM FUNCTIONAL TEST demonstrates the OPERABILITY of the initiation logic for the complete system. The system functional testing performed in other LCOs overlaps this Surveillance to provide complete testing of the assumed safety function.

The 24-month Frequency is based on the ESBWR expected refueling interval and the need to perform this Surveillance under the conditions that apply during a plant outage. The high reliability of the devices used in the signal processing coupled with the CHANNEL FUNCTIONAL TEST provides confidence that the specified Frequency is adequate.

SR 3.3.1.8.3

An OUTPUT CHANNEL FUNCTIONAL TEST is performed on each Function to ensure that the channels will operate as intended.

The Frequency of 24 months is based on the ESBWR expected refueling interval and the need to perform this Surveillance under conditions that apply during a plant outage to reduce the potential for an unplanned transient if the Surveillance was performed at power. The specified high reliability of the signal processing devices coupled with the DIVISIONAL FUNCTIONAL TEST provides confidence that the specified Frequency is adequate.

REFERENCES

1. Section 7.2.1.
2. Chapter 7, Figure 7.8-3.
3. Chapter 15.

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 Automatic Thermal Limit Monitor (ATLM) provides protection for control rod withdrawal error events. 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 and Safety Limit Minimum Critical Power Ratio (MCPR). 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 at or above the low-power setpoint (LPSP). 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. These circuits are energized when control rod movement is allowed. Control rod withdrawal is permitted only when the two channels agree. Each rod block logic circuit receives control rod position indication from a separate channel of RAPI. Control rod position and LPRM data are the primary data input for the ATLM. Average Power Range Monitor (APRM) readings are used to determine LPSP that is used to trigger the rod block function. Below the LPSP, the ATLM is automatically bypassed (Ref. 1).

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 10% RATED THEMAL POWER (RTP). The sequences enforced by 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 level signals to determine when reactor power is above the power at which the RWM is automatically bypassed (Ref. 1).

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. The reactor mode switch has four channels with each providing separate inputs into the two channels of RC&IS. A rod block in either channel will provide a control rod block to all control rods.

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

1.a. Automatic Thermal Limit Monitor (ATLM)

The ATLM is designed to prevent violation of the operating and safety limit MCPR, and the cladding 1% plastic strain fuel design limit that may result from a control rod withdrawal error (RWE) event. A summary of the RWE event assumptions used for the analysis is included in Reference 2. A statistical analysis of RWE events was performed to determine the MCPR response as a function of withdrawal distance and initial operating conditions. From these responses, some constants were derived that are used in ATLM algorithms to calculate rod block setpoints. If instantaneous Local Power Range Monitor (LPRM) data, which are fed to the ATLM, exceed the calculated rod block setpoints, a rod block signal is issued.

The Automatic 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 for plant automatic operation to ensure that no single instrument failure can preclude a rod block from this Function.

The ATLM is assumed to mitigate the consequences of a RWE event when operating above the LPSP. Below this power level, the consequences of an RWE event will not exceed the safety limit MCPR, and therefore the ATLM is not required to be OPERABLE (Ref. 3).

An Allowable Value is specified for the LPSP. The nominal setpoint is specified in procedures. The nominal setpoints are selected to ensure that the setpoints do not exceed the Allowable Values between successive CHANNEL CALIBRATIONS. Operation with a trip setpoint less conservative than the nominal trip setpoint, but within its Allowable Value, is acceptable. A channel is inoperable if its actual trip setpoint is not within its required Allowable Value. Each Allowable Value specified is more conservative than the analytical limit assumed in the transient and accident analysis in order to account for instrument uncertainties appropriate to the function. These uncertainties are described in the setpoint methodology.

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 References 4, 5, and 6. The GWSR requires that control rods be moved in groups, with all control rods assigned to a specific group required to be within specified banked positions. Requirements that the control rod sequence is in compliance with GWSR are specified in LCO 3.1.6.

The RWM Function satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii). Since the RWM is a backup to operator control of control rod sequences, or Reference Rod Pull Sequence (RRPS) for automated operation, single channel operation is allowed for manual rod movement (Ref. 6). 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 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 3.3.2.1.4 is met.

Compliance with the GWSR, and therefore OPERABILITY of the RWM, is required in MODES 1 and 2 when THERMAL POWER is ≤ 10% RTP. When THERMAL POWER is > 10% RTP, there is no possible control rod configuration that results in a control rod worth that could exceed the 280 cal/gm 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 HCU 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.

An Allowable Value is specified for the LPSP. The nominal setpoint is specified in procedures. The nominal setpoints are selected to ensure

BASES

that the setpoints do not exceed the Allowable Values between successive CHANNEL CALIBRATIONS. Operation with a trip setpoint less conservative than the nominal trip setpoint, but within its Allowable Value, is acceptable. A channel is inoperable if its actual trip setpoint is not within its required Allowable Value. Each Allowable Value specified is more conservative than the analytical limit assumed in the transient and accident analysis in order to account for instrument uncertainties appropriate to the function. These uncertainties are described in the setpoint methodology.

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).

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 GANG/SINGLE selection switch in “single”, the one rod-out interlock (LCO 3.9.2) provides the required control rod withdrawal blocks.

ACTIONS

A.1

If either ATLM channel becomes inoperable when the plant (including RC&IS) is in automatic mode of operation, RC&IS is automatically switched to the manual mode to prevent further automatic rod movement. It is required to bypass the inoperable ATLM to make it available for maintenance. The 7-day Completion Time for restoring ATLM to OPERABLE status will allow a reasonable time for trouble shooting and maintenance.

A Note permits the use of the provisions of LCO 3.0.4.c. This allowance permits entry into the applicable MODE(S) while relying on the ACTIONS. This allowance is acceptable since the RC&IS automatically switches to the manual mode preventing automatic rod movement (including automatic rod withdrawal), the probability of an event is low due to the short 7-day Completion Time, and the ability exists to restore ATLM to OPERABLE status while the plant remains at, or proceeds to power operation.

B.1

If the inoperable ATLM cannot be restored to OPERABLE status within the Completion Time of 7 days, reliability of the ATLM to initiate rod block when required is reduced. It is deemed prudent to suspend control rod withdrawal until the inoperable ATLM can be restored to OPERABLE status. Since no RWE protection is available with both ATLMs inoperable, no further rod withdrawal is allowed. Control rod withdrawal shall be suspended immediately.

C.1

If either RWM channel becomes inoperable, when the plant (including RC&IS) is in the automatic mode of operation, RC&IS is automatically switched to the manual mode to prevent further automatic rod movement. It is required to bypass the inoperable RWM to make it available for maintenance. The 7-day Completion Time for restoring RWM to OPERABLE status will allow a reasonable amount of time for trouble shooting and maintenance.

A Note permits the use of the provisions of LCO 3.0.4.c. This allowance permits entry into the applicable MODE(S) while relying on the ACTIONS. This allowance is acceptable since the RC&IS automatically switches to the manual mode preventing automatic rod movement (including automatic rod withdrawal), the probability of an event is low due to the short 7-day Completion Time, and the ability exists to restore RWM to OPERABLE status while the plant remains at, or proceeds to power operation.

D.1

If the inoperable RWM cannot be restored to OPERABLE status within 7 days, reliability of the RWM to initiate rod block when required is reduced. It is deemed prudent to suspend control rod withdrawal until the inoperable RWM can be restored to OPERABLE status. With both channels of RWMs inoperable, no RC&IS protection against RWE is available. Therefore, no further rod withdrawal is allowed. Control rod withdrawal shall be suspended immediately.

E.1

If either Rod Action Control Subsystem (RACS) cabinet becomes inoperable, when the plant (including RC&IS) is in the automatic mode of operation, RC&IS is automatically switched to the manual mode to prevent further automatic rod movement. It is required to bypass the inoperable RACS cabinet to make it available for maintenance. When a RACS cabinet becomes inoperable, all rod position monitoring, rod movement capability, and rod block functions of ATLM and RWM of the inoperable RACS cabinet are lost. Therefore, the 7-day Completion Time for restoring the inoperable RACS cabinet to OPERABLE status will allow a reasonable time for restoring the full capability of RC&IS.

F.1

If the inoperable RACS cabinet cannot be restored to OPERABLE status within 7 days, reliability of RC&IS is reduced. It is deemed prudent to suspend control rod withdrawal until the inoperable RACS cabinet can be restored to OPERABLE status. With both RACS cabinets inoperable (both channels of RC&IS inoperable), no further rod withdrawal is allowed. Control rod withdrawal shall be suspended immediately.

G.1 and G.2

If one Reactor Mode Switch - Shutdown Position control rod withdrawal block channels are inoperable, the remaining OPERABLE channels are adequate to perform the control rod withdrawal block function. Required Action G.1 and Required Action G.2 are consistent with the normal action of an OPERABLE reactor mode switch shutdown function to maintain all control rods inserted. When two or more channels become inoperable, suspending all control rod withdrawal immediately, and immediately fully insert all insertable control rods in core cells containing one or more fuel assemblies will ensure that the core is subcritical with adequate SHUTDOWN MARGIN assured by LCO 3.1.1. 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.

BASES

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.

The Surveillances are modified by a Note to indicate that an ATLM or a RWM 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 2 hours provided the associated Function maintains control rod block capability. Upon Completion of the Surveillance, or expiration of the 2-hour allowance, the channel must be returned to OPERABLE status or the applicable Condition entered and Required Actions taken.

<u>SR 3.3.2.1.1, SR 3.3.2.1.2, and SR 3.3.2.1.3</u>

The CHANNEL FUNCTIONAL TESTS for the RWM and ATLM are performed by using simulated input signals and verifying that a control rod block output occurs. This CHANNEL FUNCTIONAL TEST is performed using no actual control rod movements. If the as-found setpoint is not within its required Allowable Value the plant specific setpoint methodology may be revised, as appropriate, if the history and all other pertinent information indicates a need for the revision. The setpoint shall be left set consistent with the assumptions of the current plant-specific setpoint methodology. As noted, the SRs are not required to be performed until 1 hour after the specified conditions (e.g., after any control rod is withdrawn in MODE 2). This allows entry into the appropriate conditions needed to perform the required SRs. The Surveillance Frequencies are based on reliability analysis (Ref. 7).

<u>SR 3.3.2.1.4</u>

The LPSP is the point at which the RC&IS makes the transition between the function of the RWM and the ATLM. This power level is based upon reactor thermal power. These power setpoints must be verified periodically to be within the Allowable Values. If any LPSP is nonconservative, then the affected Functions are considered inoperable.

<u>SR 3.3.2.1.5</u>

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.

BASES

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 can not be performed without using jumpers, lifted loads or moveable limits. This allows entry into MODES 3, 4, 5, and 6 if the 24-month frequency is not met per SR 3.0.2.

The 24-month Surveillance Frequency was developed considering it is prudent that the surveillance only be performed during a plant outage. This is due to the plant conditions needed to perform the surveillance and the potential for unplanned plant transients if the surveillance is performed with the reactor at power. Operating experience has shown these components usually pass the surveillance when performed at the 24-month frequency.

SR 3.3.2.1.6

LCO 3.1.3 and LCO 3.1.6 may require individual control rods to be bypassed in the RACS 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 RACS 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.

REFERENCES

1. Section [7.1.].

2. Section [5.4.]

3. NEDE-24011-P-A-9-US, “General Electrical Standard Application for Reload Fuel,” Supplement for United States, Section S 2.2.3.1, September 1988.

4. “Modifications to the Requirements for Control Rod Drop Accident Mitigating Systems,” BWR Owners’ Group, July 1986.

5. NEDO-21231, “Banked Position Withdrawal Sequence,” January 1977.

BASES

6. NRC SER, "Acceptance of Referencing of Licensing Topical Report NEDE-24011-P-A," General Electric Standard Application for Reactor Fuel, Revision 8, Amendment 17," December 27, 1987.

7. NEDC-30851-P-A, "Technical Specification Improvement Analysis for BWR Control Rod Block Instrumentation," October 1988.

B 3.3 INSTRUMENTATION

B 3.3.3.1 Post-Accident Monitoring (PAM) Instrumentation

BASES

BACKGROUND

The primary purpose of the Post-Accident Monitoring Instrumentation is to display plant variables that provide information required by the control room operators during accident situations. This information provides the necessary support for the operator to take the manual actions for which no automatic control is provided and that are required for safety systems to accomplish their safety functions for design basis events. The instruments that monitor these variables are designated as Type A, Category 1 and non-Type A, Category 1 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 so that the control room operating staff can:

- Perform the diagnosis specified in the Emergency Operating Procedures (EOP). These variables are restricted to preplanned actions for the primary success path of Design Basis Accidents, (e.g., Loss of Coolant Accident); and

- Take the specified, preplanned, manually controlled actions for which no automatic control is provided, which are required for safety systems to accomplish their safety function.

The PAM Instrumentation LCO also ensures OPERABILITY of Category 1, non-Type A, variables. This ensures the control room operating staff can:

- Determine whether systems important to safety are performing their intended functions;

- Determine the potential for causing a gross breach of the barriers to radioactivity release;

- Determine whether a gross breach of a barrier has occurred; and

BASES

- Initiate action necessary to protect the public and to obtain estimate of the magnitude of any impending threat.

The Regulatory Guide 1.97 analysis (Ref. 2) documents the process that identified Type A and Category 1, non-Type A, variables.

PAM instrumentation that satisfies the definition of Type A in Regulatory Guide 1.97 meets Criterion 3 of 10 CFR 50.36(c)(2)(ii). Category 1, non-type A instrumentation is retained in Technical Specifications because they are intended to assist operators in minimizing the consequences of accidents (Ref. 2). Therefore, these Category 1, non-Type A variables are important for reducing public risk.

LCO

LCO 3.3.3.1 requires two OPERABLE channels for all but one Function to ensure no single failure prevents the operators from being presented with the information necessary to determine the status of the unit and to bring the unit to, and maintain it in, a safe condition following that accident.

Furthermore, provisions of two channels allows a CHANNEL CHECK during the post accident phase to confirm the validity of displayed information.

The exception of the two-channel requirement is containment isolation valve position. In this case, the important information is the status of the containment penetrations. The LCO requires one position indicator for each active containment isolation valve. This is sufficient to redundantly verify the isolation status of each isolable penetration either via indicated status of the active valve and prior knowledge of passive valve or via system boundary status. If a normally active containment isolation valve is known to be closed and deactivated, position indication is not needed to determine status. Therefore, the position indication for valves in this state is not required to be OPERABLE.

Listed below is a discussion of the specified instrument Functions listed in Table 3.3.3.1-1, in the accompanying LCO.

1. Reactor Steam Dome Pressure

Reactor steam dome pressure is a Category 1 variable provided to support monitoring of Reactor Coolant System (RCS) integrity and to verify the ADS operation of the Emergency Core Cooling System (ECCS).

BASES

Four independent pressure transmitters with a range of 0 to 10.34 MPa gauge (0 to1500 psig) monitor pressure. Wide-range displays are the primary indication used by the operator during an accident. Two of the four channels are required to be OPERABLE to satisfy the LCO. Therefore, the PAM specification deals specifically with this portion of the instrument channel.

2. and 3. Reactor Vessel Water Level

Reactor vessel water level is a Category 1 variable provided to support monitoring of core cooling and to verify operation of the ECCS. The Wide Range water level channels and the Fuel Zone water level channels provide the PAM reactor vessel water level function. The Wide Range water level channels measure from top of the active fuel to centerline of the main steam lines. Wide range water level is measured by four independent differential pressure transmitters. Four channels of Fuel Zone water level instruments cover the range from bottom of the core support plate to the top of the steam separator shroud. The output from these channels is provided to a display controller that provides a continuous display of reactor water level. These displays are the primary indication used by the operator during an accident. Two channels of Wide Range water level and two channels of Fuel Zone water level are required to be OPERABLE to satisfy the LCO requirements. Therefore, the PAM specification deals specifically with this portion of the instrument channels.

4. Suppression Pool Water Level

Suppression pool water level is a Category 1 variable provided to detect a breach in the reactor coolant pressure boundary (RCPB). This variable is also used to verify and provide long-term surveillance of ECCS function. The wide range suppression pool water level measurement provides the operator with sufficient information to assess the status of the RCPB. The wide range water level indicators monitor the suppression pool level from the bottom of the pool to 1.5 m above normal water line. Four wide range suppression pool water level signals are transmitted from separate differential pressure transmitters and are continuously displayed in the control room. Two of the four channels are required to be OPERABLE to satisfy the LCO. These displays are the primary indication used by the operator during an accident. Therefore, the PAM specification deals specifically with this portion of the instrument channel.

5. Drywell Pressure

Drywell pressure is a Category 1 variable provided to detect breach of the RCPB and to verify ECCS functions that operate to maintain RCS integrity. Four wide range drywell pressure signals are transmitted from separate pressure transmitters and are continuously displayed in the main control room. These displays are the primary indication used by the operator during an accident. Two of the four channels are required to be OPERABLE to satisfy the LCO. Therefore, the PAM specification deals specifically with this portion of the instrument channel.

6. and 7. Drywell/Wetwell Area Radiation (High Range)

Drywell and wetwell radiation measurements and displays are provided to monitor for the potential of significant radiation releases and to provide release assessment for use by operators in determining the need to invoke site emergency plans. Two separate divisions of instrumentation are provided with both drywell and wetwell monitor channels. Drywell and wetwell radiation are continuously displayed in the MCR. These displays are the primary indication used by the operator during an accident. Therefore, the PAM Specification deals specifically with this portion of the instrument channel.

8. Primary Containment Isolation Valve (PCIV) Position

PCIV position is provided for verification of containment integrity. In the case of PCIV position, the important information is the status of the containment penetration. The LCO requires one channel of valve position indication in the control room to be OPERABLE for each active PCIV in a containment penetration flow path, i.e., two total channels of PCIV position indication for a penetration flow path with two active valves. For containment penetrations with only one active PCIV having control room indication, Note (b) requires a single channel of valve position indication to be OPERABLE. This is sufficient to redundantly verify the isolation status of each isolable penetration via indicated status of the active valve, as applicable, and prior knowledge of passive valve or system boundary status. If a penetration flow path is isolated, position indication for the PCIV (s) in the associated penetration flow path is not needed to determine status. Therefore, the position indication for valves in an isolated penetration flow path is not required to be OPERABLE. Each penetration is treated separately and each penetration flow path is considered a separate function. Therefore, separate Condition entry is allowed for each inoperable penetration flow path.

Indication of the successful completion of the containment isolation safety function is provided by valve closed/not closed indicators for individual valves. This indication is provided in safety-related video display units.

9. and 10. Neutron Flux

Wide-range neutron flux is a Category 1 variable provided to verify reactor shutdown. Four separate divisions of Startup Range Neutron Monitors (SRNMs) and Average Power Range Monitors (APRMs) are provided for monitoring of neutron flux from 1E-6% RTP to 125% RTP. Two channels each of SRNM and APRM are provided for the wide-range neutron flux monitoring function. The SRNM and APRM signals are transmitted from separate SRNM and APRM channels from the Neutron Monitoring System (NMS) and are processed by the display controller and displayed in the main control room. The display controller provides a continuous display of neutron flux. These displays are the primary indication used by the operator during an accident. Therefore, the PAM specification deals specifically with this portion of the instrument channel.

11. Wetwell Pressure

Wetwell pressure is a Category 1 variable provided to detect breach of the RCPB and to verify ECCS functions that operate to maintain RCS integrity. Four wide range wetwell pressure signals are transmitted from separate pressure transmitters and are continuously displayed in the main control room. These displays are the primary indication used by the operator during an accident. Two of the four channels are required to be OPERABLE to satisfy the LCO. Therefore, the PAM specification deals specifically with this portion of the instrument channel.

12. and 13. Drywell Water Level

Drywell Water Level displays are Category 1 instruments provided for early detection of small leaks in the containment and as an alternate to drywell pressure and drywell radiation Functions. There are two channels of both upper and lower Drywell Water Level with displays and alarms provided in the MCR. These displays are the primary indication used by the operator during an accident. Therefore, the PAM Specification deals specifically with this portion of the instrument channel.

APPLICABILITY

The PAM Instrumentation LCO is applicable in MODES 1 and 2. These variables are related to the diagnosis and pre-planned 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. For the SRNM, it is not required to be OPERABLE in MODE 1 for the PAM function since the APRM will provide the necessary neutron flux monitoring in MODE 1.

ACTIONS

Two Notes have been added to the ACTIONS Table. Note 1 excludes the MODE change restriction of LCO 3.0.4. This exception allows entry into the applicable MODE while relying on the ACTIONS even though the ACTIONS may eventually require plant shutdown. This exception is acceptable due to the passive function of the instruments, the operator's ability to monitor an accident using alternate instruments and methods, and the low probability of an event requiring these instruments. A Note has been provided to modify 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 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, a Note has been provided that allows separate Condition entry for each inoperable PAM Function.

A.1

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

B.1

This Required Action specifies initiation of actions in Specification [5.6.7, "Post Accident Monitoring Report,"] which requires a written report to be submitted to the NRC. This report discusses the results of the root cause evaluation of the inoperability and identifies proposed restorative 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

When one or more Functions have two required channels inoperable, (i.e., two channels inoperable in the same Function) one channel in the Function should be restored to OPERABLE status within 7 days. The Completion Time of 7 days is based on the relatively low probability of an event requiring PAM instrument operation and the availability of alternate means to obtain the required information. Continuous operation with two required channels inoperable in a Function is not acceptable because the alternate indications may not fully meet all performance qualification requirements applied to the PAM instrumentation. Therefore, requiring restoration of one inoperable channel of the Function limits the risk that the PAM function will be in a degraded condition should an accident occur.

D.1

This Required Action directs entry into the appropriate Condition referenced in Table 3.3.3.1-1. The applicable Condition referenced in the Table is Function dependent. Each time an inoperable channel has not meet the Required Action of Condition C, and the associated Completion Time has expired, Condition D is entered for that channel and provides for transfer to the appropriate subsequent Condition.

E.1

For the majority of Functions in Table 3.3.3.1-1, if the Required Action and associated Completion Time of Condition C is not met, the plant must be placed in a MODE in which 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.

F.1

Since alternate means of monitoring primary containment and wetwell area radiation have been developed and tested, the Required Action is

BASES

not to shut down the plant but rather to follow the directions of Specification 5.6.7. These alternate means may be temporarily installed if the normal PAM channel(s) cannot be restored to OPERABLE status within the allotted time. The report to the NRC should discuss the alternate means used, describe the degree to which the alternate means are equivalent to the installed PAM channels, justify the areas in which they are not equivalent, and provide a schedule for restoring the normal PAM channels.

SURVEILLANCE REQUIREMENTS

The following SRs apply to each PAM instrumentation Function in Table 3.3.3.1-1.

SR 3.3.3.1

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 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 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 outright channel failures 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 channel of a given function in any 31 day interval is rare. The CHANNEL CHECK supplements less formal, but more frequent, checks of channels during normal operational use of those displays associated with the required channels of this LCO.

BASES

SR 3.3.3.2

A CHANNEL CALIBRATION is performed at every 24 months. 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, "Instrumentation for Light-Water Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident," Revision 3, May 1983.

2. Section 7.5.

B 3.3 INSTRUMENTATION

B 3.3.3.2 Remote Shutdown System

BASES

BACKGROUND

The Remote Shutdown System provides the control room operator with sufficient instrumentation and controls to place and maintain the plant in a safe shutdown condition from a location other than the control room. This capability is necessary to protect against the possibility of the control room becoming inaccessible. The Remote Shutdown System provides instrumentation and controls outside the main control room to allow prompt hot shutdown of the reactor after a scram and to maintain safe conditions during hot shutdown. 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 control 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 remote shutdown panel. The individual system equipment and instrumentation that interface with the Remote Shutdown System are listed on Table 7.4-1 (Ref. 1). 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 OPERABLE, reactor cooldown is achieved through the normal heat sinks. This cooldown process can be supplemented from the Remote Shutdown System panel using the Reactor Water Cleanup/Shutdown Cooling (RWCU/SDC) System. The RWCU/SDC System provides the capability to bring the reactor from high pressure conditions to cold shutdown. Control of both RWCU/SDC trains is provided on the remote shutdown panel. The Reactor Closed Cooling Water (RCCW) System is aligned to provide cooling water to the

BASES

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 the remote shutdown panel. 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. Control of both CRD trains is provided on the remote shutdown panels. If main steam line isolation occurs, the Isolation Condenser System (ICS) automatically controls reactor pressure. Because the logic processing equipment for the ICS is located within the Reactor Building, ICS operation is not affected by an event necessitating control room evacuation, and continued operation of the isolation condensers is assumed. 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 system panels using the RWCU/SDC.

In the event that the control room becomes inaccessible, the operators can establish control at the 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 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. 2).

BASES

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

LCO

The Remote Shutdown System LCO provides the requirements for the OPERABILITY of the instrumentation and controls necessary to place and maintain the plant in MODE 3 from a location other than the control room. The instrumentation and controls required are listed in Table 7.4-1 (Ref. 1).

The controls and instrumentation are those required for:

- Decay heat removal;
- Reactor pressure vessel inventory control; and
- Safety support systems for the above functions, including plant service water, reactor component cooling water, and onsite power, including the diesel generators.

The Remote Shutdown System is OPERABLE if all instrument and control channels needed to support the remote shutdown function are OPERABLE. Only one of the two Remote Shutdown panels is required to be OPERABLE.

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

The ACTIONS are modified by two Notes. Note 1 has been provided to permit the use of the provisions of LCO 3.0.4.c. This allowance permits entry into the applicable MODE(S) while relying on the ACTIONS. This allowance is acceptable due since the Remote Shutdown System does not directly impart the operation of the plant and due to the low probability of utilizing the Remote Shutdown System.

A second Note (Note 2) 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.

A.1

Condition A addresses the situation where one or more required Functions of the Remote Shutdown System is inoperable. This includes the controls for any required Function.

The Required Action is to restore the Function (both divisions, if applicable) to OPERABLE status within 30 days. The Completion Time is based on operating experience and the low probability of an event that would require evacuation of the control room.

B.1

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.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.3.3.2.1

Performance of the CHANNEL CHECK once every 31 days ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the parameter indicated on one channel to a similar parameter on other channels. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value. Significant deviations between the instrument channels could be an indication of excessive instrument drift in one of the channels or something even more serious. A CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

Agreement criteria are determined by the plant staff based on a combination of the channel instrument uncertainties, including indication and readability. If a channel is outside the criteria, it may be an indication that the sensor or the signal processing equipment has drifted outside its limit. As specified in the Surveillance, a CHANNEL CHECK is only required for those channels that are normally energized.

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

SR 3.3.3.2.2

SR 3.3.3.2.2 verifies each required Remote Shutdown System control circuit performs the intended function. This verification is performed from the remote shutdown panel and locally, as appropriate. Operation of the equipment from the remote shutdown panel is not necessary. The Surveillance can be satisfied by performance of a continuity check. This will ensure that if the control room becomes inaccessible, the plant can be placed and maintained in MODE 3 from the remote shutdown panel and the local control stations. However, this Surveillance is not required to be performed only during a plant outage. Operating experience demonstrates that Remote Shutdown System control channels usually pass the Surveillance when performed at the 24 month Frequency.

SR 3.3.3.2.3

CHANNEL CALIBRATION is a complete check of the instrument loop and the sensor. The test verifies the channel responds to measured parameter values with the necessary range and accuracy.

The 24 month Frequency is based upon operating experience and consistency with the typical industry refueling cycle.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 19.
2. Table 7.4-1.

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 water (HCW) sump monitoring system, the drywell air cooler condensate flow monitoring, and 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 to detect reactor coolant leakage 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

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 and radioactive noble gases. 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 (Refs. 3 and 4). [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. 5). 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

The ACTIONS are modified by a Note that states that the provisions of LCO 3.0.4.c are applicable. As a result, a MODE change is allowed when LCO 3.3.4.1 is not met. This allowance is provided because other instrumentation is normally available to monitor RCS leakage and since LCO 3.4.2 will require LEAKAGE to be determined every 12 hours in MODES 1, 2, 3, and 4.

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 and B.2

With both drywell fission product monitoring channels (gaseous and particulate) 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. The 30 day Completion Time for restoration recognizes that at least one other form of leakage detection is available.

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 required drywell atmospheric monitoring system is inoperable. Consistent with SR 3.0.1, Surveillances are not required to be performed on inoperable equipment.

D.1 and D.2

With both the drywell fission product monitoring system 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

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 overall plant risk is minimized. This is accomplished by placing the plant in MODE 3 within 12 hours or remaining in MODE 4. 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.

Remaining in the Applicability of the LCO is acceptable because the plant risk in MODE 3 and MODE 4 is similar to or lower than the risk in MODE 5 and because the time spent in MODE 3 to perform the necessary repairs to restore the system to OPERABLE status will be short. Going to cold shutdown results in the loss of steam-driven systems, challenges the shutdown heat removal systems, and requires restarting the plant. However, voluntary entry into MODE 5 may be made, as it is also an acceptable low-risk state.

SURVEILLANCE REQUIREMENTS

SR 3.3.4.1

This SR requires the performance of a CHANNEL CHECK of the required drywell fission product monitoring system. The check gives reasonable confidence that the channel is operating properly. The Frequency of

BASES

12 hours is based on instrument reliability and is reasonable for detecting off normal conditions.

SR 3.3.4.2

This SR requires the performance of a CHANNEL FUNCTIONAL TEST of the required RCS leakage detection instrumentation. The test ensures that the monitors can perform their function in the desired manner. The test also verifies the alarm setpoint and relative accuracy of the instrument string. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions. The Frequency of 31 days considers instrument reliability, and operating experience has shown it proper for detecting degradation.

SR 3.3.4.3

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. [GEAP-5620, April 1968.]

4. [NUREG-75/067, October 1975.]

5. Section 5.2.5.

B 3.3 INSTRUMENTATION

B 3.3.4.2 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 to provide adequate RPV pressure reduction to preclude safety/relief valve operation, conserve RPV water level, and provide core cooling. The equipment involved with ICS is described in the Bases for LCO 3.4.6, "Isolation Condenser System (ICS)."

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;
2. RPV low water level (Level 2), with time delay;
3. RPV low low water level (Level 1); or
4. Main Steam Isolation Valve (MSIV) closure of two or more MSIVs with the reactor mode switch in the RUN position.

System controls allow the reactor operator to remote-manually initiate the ICS.

The Safety System Logic and Control (SSLC) System controls the initiation signals and logic for ICS. SSLC is designed to provide a very high degree of assurance to both ensure ICS initiation when required and prevent inadvertent initiation. The input and output trip determinations for all ICS functions are based upon a two–out–of–four logic arrangement.

Four separate channels for each Function are utilized to provide input signals for ICS logic. The hardwired transmitter signals are multiplexed by divisional [local multiplexing units (LMUs)] to the Safety System Logic Control (SSLC). Each divisional digital trip module (DTM) receives the input from the instrument in that same division and compares measured multiplexed input signals with pre-established setpoints. When the setpoint is exceeded, the DTM outputs a trip signal to microprocessor–based actuation Trip Logic Unit (TLU). The output of each divisional DTM (a trip/no-trip condition) is routed to all four divisional TLUs.

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 RPS is dependent on the OPERABILITY of the individual instrumentation channel Functions specified in Table 3.3.4.2-1. Each Function must have the required number of OPERABLE channels, with their setpoints within the specified Allowable Value, where appropriate. The actual setpoint is calibrated consistent with applicable setpoint methodology assumptions. Each channel must also respond within its assumed response time.

Allowable Values are specified for each ICS Function specified in the Table. Nominal trip setpoints are specified in the setpoint calculations. The nominal setpoints are selected to ensure the actual setpoints do not exceed the Allowable Value between successive CHANNEL CALIBRATIONS. Operation with a trip setpoint less conservative than the nominal trip setpoint, but within its Allowable Value, is acceptable. A channel is inoperable if its actual trip setpoint is not within its required Allowable Value.

Trip setpoints 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, the associated device (e.g., digital trip module) changes state. The analytic limits are derived from the limiting values of the process parameters obtained from the safety analysis. [The Allowable Values are derived from the analytic limits, corrected for calibration, process and some of the instrument errors. The trip setpoints 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 channels that must function in harsh environments as defined by 10 CFR 50.49) are accounted for.

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.

BASES

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

1. 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. The Reactor Vessel Steam Dome Pressure - High Function 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.

High reactor pressure signals are initiated from four pressure transmitters 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, and MODES 3 and 4 when < 12 hours since the reactor was critical, when considerable energy exists in the reactor coolant system.

2. Reactor Vessel Water Level - Low, Level 2

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, an ICS actuation is initiated at Level 2, with a 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. The ICS actuation provides makeup water and, along with the actions of the Emergency Core Cooling System (ECCS), assures that the fuel peak cladding temperature remains below the limits of 10 CFR 50.46.

Reactor Vessel Water Level - Low, Level 2, signals are initiated from four Wide Range level transmitters 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 2, Function arranged in a two-out-of-four logic 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 and 2, and MODES 3 and 4 when < 12 hours since the reactor was critical, when considerable energy exists in the reactor coolant system.

3. Reactor Vessel Water Level – Low 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. Therefore, ICS receives the signals necessary for initiation from this Function. The Reactor Vessel Water Level - Level 1 is one of the Functions assumed to be OPERABLE and capable of actuating the ICS during the accidents analyzed in References 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 – Level 1 signals are initiated from four Wide Range level transmitters 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.

Four channels of Reactor Vessel Water Level – Level 1 Function are required to be OPERABLE when ICS is required to be OPERABLE to ensure that in case one channel has to be placed in bypass, no single instrument failure can preclude ICS actuation, when required.

4. 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 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 analyzed in Reference 1, (e.g., low steam line pressure, manual closure of MSIVs, [high steam line flow]). The ICS actuation, along with the reactor scram, assures that the fuel peak cladding temperature remains below the limits of 10 CFR 50.46.

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 isolation valve and two position switches are mounted on the outboard isolation valve. Each of the two position switches on any one MSL isolation valve is associated with a different ICS 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 an ICS initiation to occur.

The MSIV - Closure (per Steam Line) 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.

Three channels of MSIV - Closure Function (per Steam Line) 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.

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.

A.1

With one or more Function with one or more required ICS instrumentation channels inoperable, the affected instrument division must be placed in trip. Because of the diversity of sensors available to provide trip signals and the redundancy of the ICS design, an allowable out of service time of 12 hours is considered acceptable to permit restoration of any inoperable channel to OPERABLE status. However, this out of service time is only acceptable provided the associated Function still maintains ICS initiation capability (refer to Required Actions B.1 Bases). If the inoperable channel cannot be restored to OPERABLE status within the allowable out of service time, the affected instrument division must be placed in trip. Placing the ICS division in trip would conservatively compensate for the inoperability and allow operation to continue. Alternately, if it is not desired to place the ICS division in trip (e.g., as in the case where placing the ICS division in trip would result in an ICS initiation, Condition C must be entered and its Required Action taken. Most repairs are likely to be simple card or other electronic subassembly replacements that can be done on-line with the affected division of sensors in bypass. In such cases, restoration should be done as soon as practicable.

B.1

Required Action B.1 is intended to ensure that appropriate actions are taken if multiple, inoperable, untripped channels (i.e., three or more channels for most Functions) for the same Function result in the Function not maintaining ICS initiation capability. A Function is considered to be maintaining ICS initiation 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. For the typical Function with two-out-of-four logic, this would require two channels to be OPERABLE or in trip (instrument division in trip). For Function 4 (Main Steam Isolation Valve - Closure (Per Steam Line), this would require the logic to have each channel associated with the MSIVs in three MSLs (not necessarily the same MSLs), OPERABLE or in trip (instrument division in trip).

The Completion Time provides sufficient time to evaluate and repair any discovered inoperabilities. The 1 hour Completion Time is acceptable because it minimizes risk while allowing time for restoration or tripping of channels.

C.1

If an inoperable ICS instrument channel cannot be restored to OPERABLE status within the associated Completion Times of Conditions A or B, 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 operating experience, to reach the required unit conditions from full power conditions in an orderly manner and without challenging plant systems.

BASES

SURVEILLANCE REQUIREMENTS

The Surveillance Requirements are modified by two Notes. Note 1 indicates that the SRs for each ICS instrumentation Function are located in the SRs column of Table 3.3.4.2-1.

Note 2 indicates that a 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 or up to 6 hours provided the associated Function maintains trip capability. Upon completion of the Surveillance, or expiration of the 6 hour allowance, the channel must be returned to OPERABLE status or the applicable Condition entered and Required Actions taken. This Note is based on the assumption that 6 hours is the average time required to perform channel surveillance. The 6 hour testing allowance does not significantly reduce the probability that the RPS will trip when necessary.

SR 3.3.4.2.1

Performance of the CHANNEL CHECK once every 24 hours ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the parameter indicated on one channel to a similar parameter on other channels. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value. Significant deviations between the instrument channels could be an indication of excessive instrument drift in one of the channels or something even more serious. A CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

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

The Frequency is based upon 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 channels required by the LCO.

SR 3.3.4.2.2

A CHANNEL FUNCTIONAL TEST is performed on each required channel to ensure that the entire channel will perform the intended function.
Any setpoint adjustment shall be consistent with the assumptions of the current plant specific setpoint methodology.

BASES

The Frequency of [184 days] is based on the reliability and self monitoring capability of the ICS System instrumentation channels.

SR 3.3.4.2.3

A CHANNEL CALIBRATION is a complete check of the instrument loop and the sensor. This test verifies the channel responds to the measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drifts between successive calibrations consistent with the plant specific setpoint methodology.

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. Chapter 15.

B 3.3 INSTRUMENTATION

B 3.3.4.3 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 to provide adequate RPV pressure reduction to preclude safety/relief valve operation, conserve RPV water level, and provide core cooling. These actions ensure that fuel is adequately cooled in the event of a design basis transient or accident A detailed description of the ICS actuation instrumentation is provided in the Bases for LCO 3.3.4.2, “Isolation Condenser System (ICS) Instrumentation.”
APPLICABLE SAFETY ANALYSES	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).
LCO	The LCO requires four Divisions of ICS Actuation logic to be OPERABLE.
APPLICABILITY	The ICS Actuation is required to be OPERABLE in MODES 1, 2, 3, and 4 to preclude actuation of safety/relief valves and limit the peak RPV pressure to less than the ASME Section III Code limits. Additionally, ICS 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.
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

BASES

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.

A.1 and A.2

If one ICS actuation division inoperable for one or more ICS functions is inoperable, the remaining channels or divisions are sufficient to initiate ICS when required even with an additional single failure. Therefore, the inoperable division is placed in bypass. With an inoperable division in bypass, the automatic ICS logic reverts to a two–out–of–three logic, which is an acceptable long–term condition.

The Completion Time for restoring the inoperable instrument channel or division to OPERABLE status is specified for a maximum time corresponding to the refueling interval. This is acceptable because a single failure will not cause or prevent an ICS actuation when one channel of any function or one instrument division is in bypass. However, an inoperable channel or division should be restored to OPERABLE status as soon as practicable because most repairs will involve only electronic card changes or transmitter replacement.

The instrument trip channel division is not placed in trip status because that condition would satisfy half of the two–out–of–four ICS actuation. This status is avoided because it increases the potential for inadvertent ICS actuation.

B.1

If two ICS actuation divisions inoperable for one or more ICS functions, the remaining divisions are sufficient to initiate ICS when required. However, in this status, the ability to tolerate a single failure may be lost. Therefore, one channel and instrumentation division must be restored to OPERABLE status within [12] hours. The completion Time is acceptable because of the reliability of the remaining channels. Since most repairs will involve only electronic card changes or transmitter replacement, the Completion Time specified is reasonable and is not expected to impose an unnecessary burden on the plant maintenance staff.

BASES

C.1

If inoperable channels or instrument divisions result in a loss of ICCS actuation capability, ICS actuation capability must be restored to OPERABLE within one hour.

D.1

If the Required Actions and associated Completion Times of Condition A, B or C are not met, the plant must be placed in a MODE in which overall plant risk is minimized. This is accomplished by placing the plant in MODE 3 within 12 hours or remaining in MODE 4. 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.

Remaining in the Applicability of the LCO is acceptable because the plant risk in MODE 3 and MODE 4 is similar to or lower than the risk in MODE 5 (Ref. 2) and because the time spent in MODE 3 to perform the necessary repairs to restore the system to OPERABLE status will be short. Going to cold shutdown results in the loss of steam-driven systems, challenges the shutdown heat removal systems, and requires restarting the plant. However, voluntary entry into MODE 5 may be made, as it is also an acceptable low-risk state.

SURVEILLANCE REQUIREMENTS

The Surveillance Requirements are modified a Note, that indicates that a 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 or up to 6 hours provided the associated Function maintains trip capability. Upon completion of the Surveillance, or expiration of the 6 hour allowance, the channel must be returned to OPERABLE status or the applicable Condition entered and Required Actions taken. This Note is based on the assumption that 6 hours is the average time required to perform channel surveillance. The 6 hour testing allowance does not significantly reduce the probability that the ICS will actuate when necessary.

SR 3.3.4.3.1

The LOGIC SYSTEM FUNCTIONAL TEST demonstrates the OPERABILITY of the required ICS logic for a specific channel. The Surveillance Frequency at the 24 month was developed considering it is prudent that the Surveillance be performed only during a plant outage.

BASES

This is due to the plant conditions needed to perform the surveillance and the potential for unplanned transients if the surveillance is performed with the reactor at power. Operating experience has shown these components usually pass the Surveillance when performed at the 24 month Frequency.

[SR 3.3.4.3.2

This SR ensures that the individual channel response times are less than or equal to the maximum values assumed in the accident analysis. ICS SYSTEM RESPONSE TIME tests are conducted on a 24 month on a STAGGERED TEST BASIS. Staggered testing limits testing of one combination of two of the four channels to be tested during each test period so that the response time verification of every combination is completed in six cycles.

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

REFERENCES

1. Chapter 15.

2. [Topical Report with Technical Justification to Support Risk-Informed End States for ESBWR Plants is under development.]

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 a design basis transient or accident.

The ECCS instrumentation 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 and GDCS is described in the Bases for LCO 3.5.1, “ECCS - Operating.” The equipment involved with ICS is described in the Bases for LCO 3.4.5, “Isolation Condenser System (ICS).” The equipment involved with SLC is described in the Bases for LCO 3.1.7, “Standby Liquid Control (SLC).”

The Safety System Logic and Control (SSLC) System controls the initiation signals and logic for ECCS. SSLC 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. For the ESBWR, the diverse instrumentation and control system functions are provided by the Diverse Protection System (DPS). The DPS ensures compliance with defense-in-depth requirements and protection against common mode failures. [The DPS is not required to satisfy the assumptions in any accident analysis. Therefore, actuation of ECCS using the DPS solenoids is not required by Technical Specifications and is addressed in licensee controlled documents.]

ECCS initiating instrumentation must respond to a LOCA regardless of the location of the breach in the reactor coolant pressure boundary. Reactor vessel low water level is used to initiate ECCS because water level is the only parameter completely independent of breach location.

ECCS actuates in response to a RPV low water level [(Level 1.5) signal confirmed by either high drywell pressure or a 15 minute time delay] which starts the initiation sequence for ADS, GDCS, and [SLC]. ICS actuates in response to a RPV low water level [(Level 1.0) signal. On receipt of the Level [1.5] initiation signal and after a [10 second] confirmation time delay, the ECCS actuation logic triggers the following sequence of events:

1. [Both SLC trains actuate.]

2. [Five] of the [ten] ADS S/RVs open immediately to start reducing reactor pressure. If reactor water level remains below Level 1, the remaining [five] ADS S/RVs open after an additional 10-second time delay.

3. The eight DPVs, which are divided into four groups of two, open in the following sequence: The first group open after a [65 second] time delay. If reactor water level remains below Level 1, an additional DPV group opens every 45 seconds 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 that allows the ADS to depressurize the RPV. [A permissive generated by a Reactor Pressure – Low signal prevents GDCS actuation if the RPV has not de-pressurized.]

5. [ICS actuates when the RPV low water level [(Level 1.0) signal is received.]

6. All four squib-actuated valves in the GDCS equalizing lines, which connect the suppression pool to the RPV, after [30 minutes] if the [RPV water level is still below Level 0.5 (1 meter above TAF)]. [A permissive generated by a Reactor Pressure – Low signal prevents GDCS actuation if the RPV has not de-pressurized.]

Separate manual controls for ADS, GDCS, [ICS, and SLC] initiation are provided as backups to the automatic logic. Manual initiation sequences are similar to the sequences described above for automatic initiation except that the manual initiation signals do not have any timer delays. Manual initiation of GDCS immediately fires the squib valves in the GDCS branch secondary lines and, after a 30 minute time delay, fire the equalizing line squib valves are opened if RPV water level is below Level 0.5. Manual initiation for GDCS is possible only if RPV pressure is less than [0.689 MPa gauge (100 psig)].

The ECCS instrumentation utilizes and multiplexed RPV water level signals as inputs to the logic processing functions for ADS, GDCS, [ICS, and SLC actuation]. In addition, the ADS S/RV actuation logic is processed by discrete logic and the ADS DPV actuation logic is processed by microprocessor–based logic. Actuation logic for the squib–actuated valves in both the GDCS branch secondary lines and in the suppression pool equalizer lines are processed by microprocessor–based logic. The input and output trip determinations for all ECCS functions are based upon a two–out–of–four logic.

Input Logic Processing

[Four separate hardwired instrument channels and four separate multiplexed instrument channels are used to monitor RPV water level for ECCS.] [Four] separate Wide Range RPV water level transmitters [designated for ECCS] and four separate Fuel Zone water level transmitters are utilized to provide input signals for ECCS logic. Signals from four Wide Range and four Fuel Zone transmitters are multiplexed by divisional [local multiplexing units (LMUs)] to the Safety System Logic Control (SSLC). Each divisional digital trip module (DTM) for the DPV and GDCS function receives the input from the instrument in that same division and compares measured multiplexed input signals with pre-established setpoints. When the setpoint is exceeded, the DTM outputs a trip signal to microprocessor–based actuation trip logic unit (TLU). The output of each divisional DTM (a trip/no-trip condition) is routed to all four divisional DPV/GDCS Trip Logic Units (TLUs).

RPV water level signals from four separate Wide Range RPV water level transmitters are used as inputs to the analog trip modules (ATMs) in SSLC. Each divisional ATM for the S/RV compares the measured water level with the pre–established setpoint. When the setpoint is exceeded, the ATM outputs a trip signal to all four divisional S/RV discrete logic units (DLUs) as a diverse input to the trip logic.

Output Logic Processing

Based on a two–out–of–four logic, each divisional DPV or GDCS TLU outputs a trip signal to the DPV squib valve load drivers, a trip signal to the GDCS squib valve load drivers, and a trip signal to each divisional S/RV DLU as a diverse input (based on multiplexed water level signals) to the trip logic. Also based on a two–out–of–four logic, each divisional S/RV DLU outputs a trip signal to the S/RV load drivers, and a trip signal to each divisional DPV/GDCS TLU as a diverse input (based on hardwired water level signals) to the trip logic. In this arrangement, the DPV/GDCS TLU and the S/RV DLU provides a cross trip signal to each other. ADS S/RV actuations are also based on a two–out–of–four DLU trip signal load driver arrangement. GDCS squib valve actuations and DPV squib valve actuations are based on a two–out–of–four DPV/GDCS TLU trip signal load driver arrangement.

The load driver arrangement for actuation of a ADS S/RV, DPV squib valve, GDCS secondary branch line squib valve, suppression pool

BASES

equalizer line squib valve, SLC and ICS are given in References 2, 3, and 4, respectively.

Manual ADS initiation is accomplished by operating any two of the four divisional manual ADS control switches. GDCS manual initiation is accomplished by operating any two of the four divisional manual GDCS key lock switches.

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

The actions of the ECCS are explicitly assumed in the safety analyses of Reference 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 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. Each Function must have the required number of OPERABLE channels, with setpoints within the specified Allowable Values, where appropriate. A channel is inoperable if its actual trip setpoint is not within its required Allowable Value. The actual setpoint is calibrated consistent with applicable setpoint methodology assumptions.

Allowable Values are specified for each ECCS Function specified in the Table. Nominal trip setpoints are specified in the setpoint calculations. The nominal setpoints are selected to ensure the setpoints do not exceed the Allowable Value between CHANNEL CALIBRATIONS. Operations with a trip setpoint less conservative than the nominal trip setpoint, but within its Allowable Value, is acceptable. Trip setpoints 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, the trip modules output trip signals to the actuation logic units. The analytic limits are derived from the limiting values of the process parameters obtained from the safety analysis. The Allowable Values are derived from the analytic limits, corrected for calibration, [process] and some of the instrument errors. The Trip Setpoints 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 channels that must function in harsh environments as defined by 10 CFR 50.49) are accounted for.

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.

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 - Level 1.5 (Wide Range)

Reactor Vessel Water Level - Level 1.5 (Wide Range) is the primary signal for the initiation of the ECCS (i.e., ADS, GDCS, and [SLC]) because fuel damage could result if RPV water level is too low. The Reactor Vessel Water Level - Level [1.5] is assumed to be OPERABLE and capable of initiating the ADS, GDCS, and [SLC] during the accidents analyzed in References 2, 3, and 4. 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.

[Four] channels of Reactor Vessel Water Level – Level [1.5] Function are required to be OPERABLE when ADS, GDCS, and [SLC] is required to be OPERABLE to ensure that no single instrument failure can preclude ADS, GDCS and [SLC] initiation, when required [even if one channel is placed in bypass]. Level [1.5] signals are initiated from four Wide Range level sensors and transmitters. Each sensor is a channel with the four ECCS channels configured in a two-out-of-four logic (i.e., an actuation signal is generated by a low level signal from any two of the four channels.

Exceeding the Level [1.5] allowable value, in conjunction with either a confirmatory signal from High Drywell Pressure or a [15] minute time delay, starts the ADS initiation sequence timers, starts the GDCS injection valve timers, [and initiates SLC.]. [This signal also initiates the ICS after a time delay of [150] seconds. [If reactor level increases above Level [1.5] before the timer times out, the timer is automatically reset. Without a High Drywell Pressure signal, GDCS actuation does not proceed until water level remains below Level [1.5] for [15] minutes]. [GDCS injection actuation requires a permissive signal provided from Low Reactor Vessel Pressure

In MODES 4 and 5, the reactor is depressurized and therefore, the ADS functions (S/RVs and DPVs) are not required. However, two divisions of the GDCS function are required to be OPERABLE in MODES 4 and 5.

BASES

Refer to LCO 3.5.1, “ECCS–Operating”, and LCO 3.5.2, “ECCS–Shutdown”, for ADS and GDCS Applicability Bases.

2. Reactor Vessel Water Level – Level 0.5 (Fuel Zone)

Reactor Vessel Water Level - Level 0.5 (Wide Range) 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 ECCS Level 1.5 signal]. Level 0.5 is defined as 1 meter above the TAF.

Reactor Vessel Water Level - Level 0.5 signals are initiated from four Fuel Zone level transmitters. Each sensor is a channel with the four ECCS channels configured in a two-out-of-four logic (i.e., an actuation signal is generated by a low level signal from any two of the four channels).

3. Drywell Pressure - High

Drywell Pressure – High signal provides a permissive that bypasses the [15] minute time delay for ECCS actuation following a Reactor Vessel Water Level [1.5] (Wide Range) signal. This signal provides independent confirmation of a LOCA. Drywell Pressure – High consists of the four drywell pressure channels configured in a two-out-of-four logic (i.e., an actuation signal is generated by a high pressure signal from any two of the four channels.

4. RPV Pressure—Low

RPV Pressure—Low provides a permissive for actuation of GDCS injection and GDCS equalizing valves following a low reactor vessel water level signal. This permissive signal prevents GDCS actuation if the RPV has not de-pressurized. RPV Pressure—Low consists of the four RPV pressure channels configured in a two-out-of-four logic (i.e., an actuation signal is generated by a low pressure signal from any two of the four channels. These signals are multiplexed by the Local Multiplexing Units (LMUs) to Safety System and Logic Control (SSLC).

The expected containment pressure after a LOCA is approximately [30] psia. The GDCS pool injection head is approximately [20] psi. Therefore, GDCS will begin to inject into the RPV at approximately 50 psia reactor pressure. The Allowable Value for the pressure permissive is chosen so that the squib valves are fired prior to reaching the reactor pressure at which GDCS can inject into the RPV.

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 and A.2

If one instrument trip channel (input logic processing) in one or more Functions [or an instrument division] becomes inoperable, the inoperable channel [or division] is placed in bypass status. With an inoperable channel [or instrument division] in bypass status, the automatic ECCS logic reverts to a two–out–of–three logic, which is an acceptable long–term condition.

The Completion Time for restoring the inoperable instrument channel or division to OPERABLE status is specified for a maximum of time corresponding to the refueling interval. This is acceptable because a single failure will not cause or prevent an ECCS actuation when one channel of any function or one instrument division is in bypass. However, an inoperable channel or division should be restored to OPERABLE status as soon as practicable because most repairs will involve only electronic card changes or transmitter replacement.

The instrument trip channel [or instrument division] is not placed in trip status because that condition would satisfy half of the two–out–of–four ECCS actuation. This status is avoided because it increases the potential for inadvertent ECCS actuation.

B.1

If one or more Functions have two required ECCS instrumentation channels or instrumentation divisions inoperable, the remaining channels or divisions are sufficient to initiate ECCS when required. However, in this status, the ability to tolerate a single failure may be lost. Therefore, one channel and instrumentation division must be restored to OPERABLE status within [12] hours. The completion Time is acceptable because of the reliability of the remaining channels. Since most repairs will involve only electronic card changes or transmitter replacement, the Completion Time specified is reasonable and is not expected to impose an unnecessary burden on the plant maintenance staff.

C.1

If inoperable channels or instrument divisions result in a loss of ECCS actuation capability, ECCS actuation capability must be restored to OPERABLE within one hour.

D.1

If the Required Actions and associated Completion Times of Condition A, B or C are not met, the plant must be placed in a MODE in which overall plant risk is minimized. This is accomplished by placing the plant in MODE 3 within 12 hours or remaining in MODE 4. 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.

Remaining in the Applicability of the LCO is acceptable because the plant risk in MODE 3 and MODE 4 is similar to or lower than the risk in MODE 5 (Ref. 5) and because the time spent in MODE 3 to perform the necessary repairs to restore the system to OPERABLE status will be short. Going to cold shutdown results in the loss of steam-driven systems, challenges the shutdown heat removal systems, and requires restarting the plant. However, voluntary entry into MODE 5 may be made, as it is also an acceptable low-risk state.

SURVEILLANCE REQUIREMENTS

The Surveillance Requirements are modified by two Notes. Note 1 indicates that the SRs for each ICS instrumentation Function are located in the SRs column of Table 3.3.5.1-1.

Note 2 indicates that a 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 or up to [6] hours provided the associated Function maintains trip capability.

Upon Completion of the Surveillance, or expiration of the [6] hour allowance, the channel must be returned to OPERABLE status or the applicable Condition entered and Required Actions taken. This Note is based on the reliability analysis assumption that 6 hours is the average time required to perform channel Surveillance. That analysis demonstrated that the 6 hour testing allowance does not significantly reduce the probability that the ECCS will initiate when necessary.

SR 3.3.5.1.1

Performance of the CHANNEL CHECK once every 24 hours ensures that a gross failure of instrumentation has not occurred. Performance of this check provides confidence that a gross failure of a device in a sensor channel has not occurred. This check is a visual comparison on the MCR main control console.

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 instrument channels could be an indication of excessive instrument drift in one of the channels or something even more serious. A CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying that the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

Agreement criteria are determined by the plant staff, based on a combination of the channel instrument uncertainties, including indication and readability. If a channel is outside the 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. Thus, performance of the CHANNEL CHECK guarantees that undetected outright channel failure is limited to 12 hours. The CHANNEL CHECK supplements less formal, but more frequent checks of channels during normal operational use of the displays associated with the LCO's required channels.

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 functional test provides confidence that the software-based control programs within the SSLC controllers perform as intended. The test is performed by replacing the process signal with a test signal, which is generated by the SSLC test controller instrument. This test checks the function of the digital trip function and checks trip logic and interlock logic response. This functional test is performed on-line with a sensor channel or logic channel bypassed. This test is semi-automatic and supplements

BASES

the continuous self-diagnostic checks within each SSLC controller If the as-found setpoint is not within its required Allowable Value, the plant specific setpoint methodology may be revised, as appropriate if the history and all other pertinent information indicate a need for the revision. The setpoint shall be left consistent with the assumptions of the current plant-specific setpoint methodology.

<u>SR 3.3.5.1.3</u>

A CHANNEL CALIBRATION is a complete check of the instrument loop and the sensor. This test verifies the channel responds to the measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drifts between successive calibrations consistent with the plant specific setpoint methodology.

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.

<u>SR 3.3.5.1.4</u>

This SR ensures that the individual channel response times are less than or equal to the maximum values assumed in the accident analysis. ECCS RESPONSE TIME tests are conducted on a 24 month on a STAGGERED TEST BASIS. Staggered testing limits testing of one combination of two of the four channels to be tested during each test period so that the response time verification of every combination is completed in six cycles.

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

REFERENCES

1. Chapter 6.
2. Chapter 7.
3. Chapter 5.
4. Chapter 15.

BASES

5. [Topical Report with Technical Justification to Support Risk-Informed End States for ESBWR Plants is under development.]

B 3.3 INSTRUMENTATION

B 3.3.5.2 EMERGENCY CORE COOLING SYSTEM (ECCS) ACTUATION

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 a design basis transient or accident. The ECCS instrumentation 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 and GDCS is described in the Bases for LCO 3.5.1, "ECCS - Operating." The equipment involved with ICS is described in the Bases for LCO 3.4.5, "Isolation Condenser System (ICS)." The equipment involved with SLC is described in the Bases for LCO 3.1.7, "Standby Liquid Control (SLC)." A detailed description of the ECCS actuation instrumentation is provided in the Bases for LCO 3.3.5.1, "Emergency Core Cooling System (ECCS) Instrumentation."
APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY	The ECCS signals generated by the ECCS instrumentation are implicitly assumed in the safety analyses of References 1 and 2 to initiate closure of valves to limit off-site doses. ECCS Actuation 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. Each Function must have the required number of OPERABLE channels, with setpoints within the specified Allowable Values, where appropriate. A channel is inoperable if its actual trip setpoint is not within its required Allowable Value. The actual setpoint is calibrated consistent with applicable setpoint methodology assumptions.
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

If one ECCS actuation division inoperable for one or more ECCS functions is inoperable, the remaining channels or divisions are sufficient to initiate ECCS when required even with an additional single failure. Therefore, the inoperable division is place in bypass. With an inoperable division in bypass status, the automatic ECCS logic reverts to a two–out–of–three logic, which is an acceptable long–term condition.

The Completion Time for restoring the inoperable instrument channel or division to OPERABLE status is specified for a maximum of time corresponding to the refueling interval. This is acceptable because a single failure will not cause or prevent an ECCS actuation when one channel of any function or one instrument division is in bypass. However, an inoperable channel or division should be restored to OPERABLE status as soon as practicable because most repairs will involve only electronic card changes or transmitter replacement.

The instrument trip channel division is not placed in trip status because that condition would satisfy half of the two–out–of–four ECCS actuation. This status is avoided because it increases the potential for inadvertent ECCS actuation.

B.1

If two ECCS actuation divisions inoperable for one or more ECCS functions, the remaining divisions are sufficient to initiate ECCS when required. However, in this status, the ability to tolerate a single failure may be lost. Therefore, one channel and instrumentation division must be restored to OPERABLE status within [12] hours. The completion Time is acceptable because of the reliability of the remaining channels. Since most repairs will involve only electronic card changes or transmitter replacement, the Completion Time specified is reasonable and is not expected to impose an unnecessary burden on the plant maintenance staff.

C.1

If inoperable channels or instrument divisions result in a loss of ECCS actuation capability, ECCS actuation capability must be restored to OPERABLE within one hour.

D.1

If the Required Actions and associated Completion Times of Condition A, B or C are not met in Modes 1, 2 or 3, the plant must be placed in a MODE in which overall plant risk is minimized. This is accomplished by placing the plant in MODE 3 within 12 hours or remaining in MODE 4. 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.

Remaining in the Applicability of the LCO is acceptable because the plant risk in MODE 3 and MODE 4 is similar to or lower than the risk in MODE 5 (Ref. 5) and because the time spent in MODE 3 to perform the necessary repairs to restore the system to OPERABLE status will be short. Going to cold shutdown results in the loss of steam-driven systems, challenges the shutdown heat removal systems, and requires restarting the plant. However, voluntary entry into MODE 5 may be made, as it is also an acceptable low-risk state.

E.1

If the Required Actions and associated Completion Times of Condition A, B or C are not met in Modes 4, 5 or 6, the associated ECCS component must be declared inoperable.

SURVEILLANCE REQUIREMENTS

The Surveillance Requirements are modified by two Notes. Note 1 indicates that the SRs for each ICS instrumentation Function are located in the SRs column of Table 3.3.5.1-1.

Note 2 indicates that a 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 or up to [6] hours provided the associated Function maintains trip capability.

Upon Completion of the Surveillance, or expiration of the [6] hour allowance, the channel must be returned to OPERABLE status or the applicable Condition entered and Required Actions taken. This Note is based on the reliability analysis assumption that 6 hours is the average time required to perform channel Surveillance. That analysis demonstrated that the 6 hour testing allowance does not significantly reduce the probability that the ECCS will initiate when necessary.

SR 3.3.5.2.1

The LOGIC SYSTEM FUNCTIONAL TEST demonstrates the OPERABILITY of the required ECCS logic for a specific channel. The Surveillance Frequency at the 24 month for SR 3.3.5.2. was developed considering it is prudent that the Surveillance be performed only during a plant outage.

This is due to the plant conditions needed to perform the surveillance and the potential for unplanned transients if the surveillance is performed with the reactor at power. Operating experience has shown these components usually pass the Surveillance when performed at the 24 month Frequency.

[SR 3.3.5.2.2

This SR ensures that the individual channel response times are less than or equal to the maximum values assumed in the accident analysis. ECCS RESPONSE TIME tests are conducted on a 24 month on a STAGGERED TEST BASIS. Staggered testing limits testing of one combination of two of the four channels to be tested during each test period so that the response time verification of every combination is completed in six cycles.

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

REFERENCES

1. Chapter 6.
2. Chapter 7, Figure 7.
3. Chapter 5.
4. Chapter 15.

BASES

5. [Topical Report with Technical Justification to Support Risk-Informed End States for ESBWR Plants is under development.]

B 3.3 INSTRUMENTATION

B 3.3.6.1 Isolation Instrumentation

BASES

BACKGROUND

The isolation instrumentation contained in this specification provides the capability to generate isolation signals to the following systems:
(1) containment isolation (including the main steam and drain lines, isolation condenser, reactor water cleanup/shutdown cooling lines, fission product sampling lines, drywell low conductivity waste sump drain line, drywell high conductivity waste sump drain line, containment purge and vent valves, reactor component cooling water valves to the drywell air coolers, and the fuel and auxiliary pools cooling system); (2) reactor building, (3) refueling area exhaust isolation; and (4) main control room isolation.

The isolation instrumentation automatically initiates closure of appropriate isolation valves. The function of the isolation valves, in combination with other accident mitigation systems, is to limit fission product release during and following postulated Design Basis Accidents (DBAs).

The isolation instrumentation includes the sensors, digital trip unit modules (DTMs), load drivers, bypass circuits, and switches that are necessary to isolation. The channels include electronic equipment (e.g., DTMs) that compares measured input signals with pre-established setpoints. When the setpoint is exceeded, the channel outputs an isolation signal to the isolation logic. Functional diversity is provided by monitoring a wide range of independent parameters. The input parameters to the isolation logics are (a) reactor vessel water level (Level 1 and Level 2), (b) drywell pressure, main steam line flow, condenser vacuum, main steam tunnel ambient temperature, main steam tunnel ambient temperature, reactor water cleanup/shutdown cooling subsystem flow, RWCU/SDC flow, isolation condenser steam flow, isolation condenser condensate flow, isolation condenser subsystem pool vent discharge radiation, reactor building HVAC exhaust radiation, refueling area exhaust radiation, and main control room intake radiation team flow. Redundant sensor input signals from each parameter are provided for initiation of isolation.

The isolation instrumentation contains four separate divisions of requisite instrumentation, including sensors, digital trip modules (DTMs) and switches, necessary to monitor specific plant parameters and to generate a trip signal to all four channels of the actuation logic if a predetermined value is exceeded. A actuation logic channel will in turn generate a tripped condition to both divisions of a two division trip logic system. The trip logic system will then trip the associated systems to an isolated condition state when more than one actuation signal is received. For main steam isolation valves (MSIVs) and main steam line (MSL) drains, a two-out-of-four trip in a TLU causes a trip in its corresponding Output Logic Unit (OLU). It is this trip that then initiates main steam isolation. The overall arrangement of OLU outputs and load driver for MSIV and MSL drain isolation is such that a trip of any two of four TLUs (and associated OLUs) will cause the complete closure of all MSIVs and MSL drain valves.

The other isolations are done in the Emergency Core Cooling System (ECCS) SSLC and logic for the affected system. This logic will be the same as the ECCS logic in that it will use four divisions of sensors (with a division of sensors bypass switch) and two two-out-of-four trip decision per division that each operates a LD. Although all four divisions contribute to the isolation decision, the LDs in question reside in the division in which the isolation valve is powered (usually Division 1 and Division 2). There is also (non isolation) logic in the same division to operate the valve normally (i.e., open it). These isolation LD are wired in series such that each division must make a two-out-of-two decision (the single failure for isolation is the valve in the other division). The isolation logic is further discussed in the Bases of LCO 3.3.6.1.

The containment isolation instrumentation automatically initiates closure of appropriate containment isolation valves (CIVs). The function of the CIVs, in combination with other accident mitigation systems, is to limit fission-product release during and following postulated Design Basis Accidents (DBAs). Containment isolation within the time limits specified for those isolation valves designed to close automatically ensure that the release of radioactive material to the environment will be limited and consistent with the assumptions used in the analyses for a DBA.

The input parameters to the isolation logics are (a) reactor vessel water level (Level 1 and Level 2), (b) drywell pressure, main steam line flow, condenser vacuum, main steam tunnel ambient temperature, main steam tunnel ambient temperature, reactor water cleanup/shutdown cooling subsystem flow, RWCU/SDC flow, isolation condenser steam flow, isolation condenser condensate flow, isolation condenser subsystem pool vent discharge radiation, reactor building HVAC exhaust radiation, refueling area exhaust radiation, and main control room intake radiation team flow.

BASES

The reactor building/refueling area exhaust isolation instrumentation automatically initiates closure of appropriate reactor building/refueling area exhaust isolation valves. The function of this, in combination with other accident mitigation systems, is to limit fission-product release during and following postulated Design Basis Accidents (DBAs) such that off-site radiation exposures are maintained within the requirements of 10 CFR 100 that are part of the NRC staff-approved licensing basis. Reactor building/Refueling Area Exhaust isolation ensures that fission-products that leak from containment following a DBA or are released outside containment, or that are released during certain operations when containment is not required to be OPERABLE, are maintained within applicable limits.

The input parameters to the isolation logics are (a) reactor vessel water level (Level 1 and Level 2), (b) drywell pressure, main steam line flow, condenser vacuum, main steam tunnel ambient temperature, main steam tunnel ambient temperature, reactor water cleanup/shutdown cooling subsystem flow, RWCU/SDC flow, isolation condenser steam flow, isolation condenser condensate flow, isolation condenser subsystem pool vent discharge radiation, reactor building HVAC exhaust radiation, refueling area exhaust radiation, and main control room intake radiation team flow.

The main control room (MCR) isolation instrumentation, in conjunction with the Emergency Breathing Air System (EBAS), is designed to provide a radiologically controlled environment to ensure the habitability of the MCR for the safety of operators under accident conditions for up to 72 hours, concurrent with a total Loss of Off-site Power (LOP). The two independent, redundant EBAS subsystems are each capable, by themselves, of fulfilling the stated function. The isolation instrumentation automatically initiates action to isolate the MCR to minimize the consequences of radioactive material in the MCR environment and automatically initiates the EBAS upon detection of high radiation at the MCR ventilation intake.

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

The isolation signals generated by the isolation instrumentation are implicitly assumed in the safety analyses of References 1 and 2 to initiate closure of valves to limit off-site doses.

The isolation signals generated by the reactor building and refueling area exhaust isolation instrumentation are implicitly assumed in the safety analyses to initiate closure of valves to limit off site doses.

The ability of EBAS to maintain the habitability of the MCR is explicitly assumed for certain accidents as discussed in the safety analyses. The isolation of the control room and the operation of EBAS ensures the radiation exposure of control room personnel, through the duration of any one of the postulated accidents, does not exceed the limits set by GDC 19 of 10 CFR 50, Appendix A.

Isolation instrumentation satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii). Certain monitored instrumentation parameters are retained for other reasons and are described below in the individual process parameter discussion.

The OPERABILITY of the isolation instrumentation function is dependent on the OPERABILITY of each individual process parameter monitored as specified in Table 3.3.6.1-1. Each monitored parameter must have four OPERABLE channels, with their setpoints within the specified Allowable Values, where appropriate. A channel is inoperable if its actual trip setpoint is not within its required Allowable Value. The actual setpoint is calibrated consistent with applicable setpoint methodology assumptions. Each channel must also respond within its assumed response time, where appropriate. Allowable Values are specified for each monitored process parameter specified in the Table. Nominal trip setpoints are specified in the setpoint calculations. The nominal setpoints are selected to ensure the setpoints do not exceed the Allowable Value between CHANNEL CALIBRATIONS. Operation with a trip setpoint less conservative than the nominal trip setpoint, but within its Allowable Value, is acceptable.

Trip setpoints 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, the associated device (e.g., DTM) changes state. The analytic limits are derived from the limiting values of the process parameters obtained from the safety analysis. The Allowable Values are derived from the analytic limits, corrected for calibration, process and some of the instrument errors. The Trip Setpoints 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 channels that must function in harsh environments as defined by 10 CFR 50.49) are accounted for.

BASES

In general, the individual monitored process parameters are required to be OPERABLE in the MODES or other specified conditions when Containment Integrity, Reactor building/Refueling Area Exhaust and Main Control Room isolation capability is required. The specific Applicability Requirements are specified in Table 3.3.6.1-1.

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

1. Reactor Vessel Low Water Level - 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 Function isolates the main steam and drain lines, reactor water cleanup/shutdown cooling lines, fission product sampling lines, drywell low conductivity waste sump drain line, drywell high conductivity waste sump drain line, containment purge and vent valves, reactor component cooling water valves to the drywell air coolers, and the fuel and auxiliary pools cooling system, the reactor building, and the refueling area exhaust isolation.

The valves whose penetrations communicate with the containment are isolated to limit the release of fission-products. The isolation of the containment on Level 2 supports actions to ensure that off-site dose limits of 10 CFR 100 are not exceeded. The Reactor Vessel Low Water Level - Level 2 Function associated with containment isolation is implicitly assumed in the safety analyses as these leakage paths are assumed to be isolated post-LOCA.

An isolation of the reactor building/refueling area exhaust is initiated in order to minimize the potential of an off-site dose release. The Reactor Vessel Low Water Level - Level 2 Function is one of the Functions assumed to be OPERABLE and capable of providing isolation and initiation signals. The Reactor building isolation on Reactor Vessel Low Water Level - Level 2 support actions to ensure any off-site releases are within the limits calculated in the safety analysis. However, the Reactor Vessel Low Water Level - Level 2 Function associated with reactor building isolation is not directly assumed in safety analyses because the most limiting design basis accident is a main steam line break outside the reactor building.

Reactor Vessel Low Water Level - Level 2 signals are initiated from level transmitters 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. Four channels of Reactor

Vessel Low Water Level - Level 2 Function are available and three channels are required to be OPERABLE to ensure no single instrument failure can preclude the isolation function.

The Reactor Vessel Low Water Level - Level 2 Function is required to be OPERABLE in MODES 1, 2, 3, and 4 where considerable energy exists in the reactor coolant system and thus there is a probability of pipe breaks resulting in significant releases of radioactive steam and gas. In MODES 5 and 6 it also required to be OPERABLE to isolate the Reactor Water Cleanup/Shutdown Cooling System lines in order isolate the reactor coolant system to prevent a draindown of the reactor vessel.

2. Reactor Vessel Low Water Level - Level 1

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 Function isolates the main steam and drain lines, reactor water cleanup/shutdown cooling lines, fission product sampling lines, drywell low conductivity waste sump drain line, drywell high conductivity waste sump drain line, containment purge and vent valves, reactor component cooling water valves to the drywell air coolers, and the fuel and auxiliary pools cooling system, the reactor building, and the refueling area exhaust isolation.

The valves whose penetrations communicate with the containment are isolated to limit the release of fission-products. The isolation of the containment on Level 1 supports actions to ensure that off-site dose limits of 10 CFR 100 are not exceeded. The Reactor Vessel Low Water Level - Level 1 Function associated with containment isolation is implicitly assumed in the safety analyses as these leakage paths are assumed to be isolated post-LOCA.

An isolation of the reactor building/refueling area exhaust is initiated in order to minimize the potential of an off-site dose release. The Reactor Vessel Low Water Level - Level 1 Function is one of the Functions assumed to be OPERABLE and capable of providing isolation and initiation signals. The reactor building isolation on Reactor Vessel Low Water Level - Level 1 support actions to ensure any off-site releases are within the limits calculated in the safety analysis. However, the Reactor Vessel Low Water Level - Level 1 Function associated with reactor building isolation is not directly assumed in safety analyses because the most limiting design basis accident is a main steam line break outside the reactor building.

Reactor Vessel Low Water Level - Level 1 signals are initiated from level transmitters 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. Four channels of Reactor Vessel Low Water Level - Level 1 Function are available and three channels are required to be OPERABLE to ensure no single instrument failure can preclude the isolation function.

The Reactor Vessel Low Water Level - Level 1 Function is required to be OPERABLE in MODES 1, 2, 3, and 4 where considerable energy exists in the reactor coolant system and thus there is a probability of pipe breaks resulting in significant releases of radioactive steam and gas. In MODES 5 and 6 it also required to be OPERABLE to isolate the Reactor Water Cleanup/Shutdown Cooling System lines in order to isolate the reactor coolant system to prevent a draindown of the reactor vessel.

3. Drywell Pressure - High

High drywell pressure can indicate a break in the reactor coolant pressure boundary. The Function isolates the fission product sampling lines, drywell low conductivity waste sump drain line, drywell high conductivity waste sump drain line, containment purge and vent valves, reactor component cooling water valves to the drywell air coolers, and the fuel and auxiliary pools cooling system, the reactor building, and the refueling area exhaust isolation.

The isolation of some of the containment isolation valves on high drywell pressure supports actions to ensure that off-site dose limits of 10 CFR 100 are not exceeded. The Drywell Pressure - High Function associated with isolation of the containment is implicitly assumed in the accident analysis as these leakage paths are assumed to be isolated post-LOCA.

An isolation of the Reactor building exhaust is initiated in order to minimize the potential of an off-site dose release. The isolation on high drywell pressure supports actions to ensure any off-site releases are within the limits calculated in the safety analysis. However, the Drywell Pressure—High Function associated with Reactor building isolation is not assumed in any accident or transient analyses. It is retained for the overall redundancy and diversity of the Reactor building/Refueling Area Exhaust isolation instrumentation as required by the NRC approved licensing basis.

High drywell pressure signals are initiated from pressure transmitters that sense the pressure in the drywell. Four channels of Drywell Pressure—High are available and three are required to be OPERABLE to ensure no single instrument failure can preclude the isolation function.

The Drywell Pressure-High Function is required to be OPERABLE in Modes MODES 1, 2, 3, and 4 where considerable energy exists in the reactor coolant system and thus the probability of pipe breaks resulting in significant releases of radioactive steam and gas. This Function is not required in MODES 5 and 6 because the probability and consequences of these events are low due to the reactor coolant system pressure and temperature limitations of these MODES.

<u>4. Main Steam Line Pressure - Low</u>

Low main steam line pressure indicates that there may be a problem with the turbine pressure regulation that could result in a condition that the Reactor Pressure Vessel (RPV) is cooling down more than 55°C/hr (100°F/hr) if the pressure loss is allowed to continue. The Function isolates the main steam and drain lines.

The Main Steam Line Pressure - Low Function is directly assumed in the analysis of the pressure regulator failure (Ref. 2). For this event the closure of the MSIVs ensures that the RPV temperature change limit 55°C/hr (100°F/hr) is not reached. In addition, this Function supports actions to ensure Safety Limit 2.1.1.1 is not exceeded. (This Function closes the MSIVs prior to pressure decreasing below 5.412 MPa gauge (785 psig), which results in a scram due to MSIV closure, thus reducing reactor power to < [25%] RTP.)

The main steam line low-pressure signals are initiated from four transmitters that are connected to the main steam line header. The transmitters are arranged such that, even though physically separated from each other, each transmitter is able to detect low main steam line pressure. Four channels of Main Steam Line Pressure—Low Function are available and three 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. 2).

BASES

5. Main Steam Line Flow - High

Main Steam Line Flow - High is provided to detect a break of the Main Steam Line and to initiate closure of the MSIVs. The Function isolates the main steam and drain lines. If the steam was 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 main steam line break (Ref. 2). The isolation action, along with the scram function of the RPS assures that the fuel peak cladding temperature remains below the limits of 10 CFR 50.46 and off-site doses do not exceed the 10 CFR 100 limits.

The main steam line flow signals are initiated from sixteen transmitters that are connected to the four main steam lines, four per steam line. The transmitters are arranged such that, even though physically separated from each other, all four connected to one steam line would be able to detect the high flow in that steam line. High steamline flow in any of the two steam lines will result in isolation of all steamlines.

The Main Steam Line Flow-High Function is only required to be OPERABLE in MODE 1, 2, 3, and 4 since this is when the assumed transient can occur. However, as noted, the channels are not required to be OPERABLE if the main steam line is isolated, since the channels have performed their intended function and will not be able to sense a break in a different line (since their associated line is isolated).

Four channels of Main Steam Line Flow - High Function for each unisolated main steam line are available and [three] for each unisolated 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 off-site dose limits are not exceeded due to the break.

6. Condenser Vacuum - Low

The Condenser Vacuum - Low Function is provided to prevent overpressurization of the main condenser in the event of a loss of main condenser vacuum. The Function isolates the main steam and drain lines. Since, the integrity of the condenser is an assumption in off-site dose calculations, the Condenser Vacuum-Low Function is assumed to be OPERABLE and capable of initiating closure of the MSIVs. The closure of the MSIVs 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. Condenser vacuum pressure signals are derived from four pressure transmitters that sense the pressure in the condenser. Four channels of Condenser Vacuum-Low Function are available and three 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 off-site dose analysis.

The Condenser Vacuum - Low Function is required to be OPERABLE in MODES 1, 2, 3, and 4 where considerable energy exists in the reactor coolant system and there is a potential to overpressurize the condenser. In MODES 5 and 6, the reactor is shutdown and the potential to overpressurize the condenser is low. As noted, the channels are not required to be OPERABLE in MODES 2, 3, and 4 when all turbine stop valves are closed since the potential for condenser overpressurization is minimized. [Switches are provided to manually bypass the channels when all turbine stop valves are closed.]

<u>7, 8. Main Steam Tunnel and Turbine Area Ambient Temperature - High</u>

Ambient Temperature - High is provided to detect a leak in the reactor coolant pressure boundary and provides diversity to the high flow instrumentation. The Main Steam Tunnel Ambient Temperature - High Function will isolate both Main Steam and Reactor Water Cleanup/Shutdown Cooling (RWCU/SDC) valves, while the Main Steam Turbine Area Ambient Temperature - High Function will isolate the Main Steam valves only.

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 Main Steam High Flow is more limiting for off-site doses.

Ambient temperature signals are initiated from thermocouples located in the area being monitored. Four channels of Main Steam Tunnel Temperature - High Function are available and three are required to be

OPERABLE to ensure no single instrument failure can preclude the isolation function. Each Function has one temperature element.

The ambient temperature monitoring Allowable Value is chosen to detect a leak equivalent to 1.577 l/second (25 gpm).

The Main Steam Tunnel - High and Turbine Area Ambient Temperature - High Functions are required to be OPERABLE in MODES 1, 2, 3, and 4 where considerable energy exists in the reactor coolant system and thus there is a probability of pipe breaks resulting in significant releases of radioactive steam and gas. In MODES 5 and 6, the probability and consequences of these events are low due to the reactor coolant system pressure and temperature limitations of these MODES, thus this Function is not required

9. Reactor Water Cleanup/Shutdown Cooling Subsystem Flow - High

The Reactor Water Cleanup/Shutdown Cooling (RWCU/SDC) Subsystem Flow - High signal is provided to detect a break in the RWCU system. The Function isolates the RWCU/SDC lines. 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) Subsystem - High is sensed to prevent exceeding off-site doses. This Function is not assumed in any transient or accident analysis because other leak paths (e.g., MSIVs) are more limiting.

Four channels of the (RWCU/SDC) Subsystem Flow - High Function are available and [three] are required to be OPERABLE to ensure no single instrument failure can preclude the isolation function.

The (RWCU/SDC) Subsystem Flow - High Allowable Value ensures that the break of the RWCU piping is detected.

The (RWCU/SDC) Subsystem Flow -High Function is required to be OPERABLE in MODES 1, 2, 3, and 4 where considerable energy exists in the reactor coolant system and thus there is a probability of pipe breaks resulting in significant releases of radioactive steam and gas. In MODES 5 and 6, the probability and consequences of these events are low due to the reactor coolant system pressure and temperature limitations of these MODES, thus this Function is not required.

BASES

10, 11, and 12. Isolation Condenser Steam and Condensate Line Flow - High and Pool Vent Discharge Radiation - High

The Isolation Condenser (IC) Steam Line Flow high, Condensate Line Flow - High, and Pool Vent Discharge Radiation -High Functions work together to monitor the pressure boundary status of each individual IC subsystem. These Functions isolate the IC System lines. The isolation signals can be initiated from a total of twelve instruments per IC subsystem, with each subsystem having four flow transmitters on its steam line, four flow transmitters on its condensate line and four radiation detectors located in its associated IC pool's airspace. The flow transmitters are arranged such that, even though physically separated from each other, all four connected to the steam or all four connected to the condensate line would be able to detect the high flow in that line. Four channels of each monitored parameter are available for each subsystem and three are required to be OPERABLE to ensure no single instrument failure can preclude the isolation functions.

These Functions together assure that a failure of an IC pressure boundary will be detected and isolated.

The Isolation Condenser (IC) Steam Line Flow - High, Condensate Line Flow - High and Pool Vent Discharge Radiation - High Functions are required to be OPERABLE in MODES 1, 2, 3, and 4 where considerable energy exists in the reactor coolant system and thus there is a probability of pipe breaks resulting in significant releases of radioactive steam and gas. In MODES 5 and 6, the probability and consequences of these events are low due to the reactor coolant system pressure and temperature limitations of these MODES, thus this Function is not required.

13, 14. Reactor Building HVAC Exhaust Radiation - High and Refueling Area Exhaust Radiation - High

Reactor Building HVAC Exhaust Radiation - High and Refueling Area Exhaust Radiation - High is an indication of possible gross failure of the fuel cladding. 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 HVAC Exhaust Radiation - High or Refueling Area Exhaust Radiation - High signal is detected, a reactor building/refueling area exhaust isolation is initiated to limit the release of fission products as assumed in the safety analyses (Ref. 2).

The Reactor Building HVAC Exhaust Radiation - High and Refueling Area Exhaust Radiation - High signals are initiated from radiation detectors that are located on the ventilation exhaust piping coming from the Reactor building and the Refueling Area, respectively. Four channels of Reactor building Exhaust Radiation—High Function and four channels of Refueling Area Exhaust Radiation—High Function are available and three of each are required to be OPERABLE to ensure no single instrument failure can preclude the isolation functions.

The Allowable Values are chosen to promptly detect gross failure of the fuel cladding.

The Reactor Building HVAC Exhaust Radiation - High and Refueling Area Exhaust Radiation - High Functions are required to be OPERABLE in MODES 1, 2, 3, and 4 where considerable energy exists and thus the probability of pipe breaks resulting in significant releases of radioactive steam and gas. In MODES 5 and 6, the probability and consequences of these events are low due to the reactor coolant system pressure and temperature limitations of these MODES, thus these Functions are not required. In addition, the Functions are required to be OPERABLE during operations with a potential for draining the reactor vessel and movement of irradiated fuel assemblies in the reactor building because the capability of detecting radiation releases due to fuel failures (due to fuel uncovery or dropped fuel assemblies) must be provided to ensure off-site dose limits are not exceeded.

<u>15. Main Control Room Intake Radiation - High</u>

The Control Room Ventilation Radiation Monitors measure radiation levels exterior to the inlet ducting of the MCR. A high radiation level may pose a threat to MCR personnel and thus a detector indicating this condition automatically signals to isolate the MCR and initiate the MCRBA system.

The Main Control Room Intake Radiation High Function consists of four independent monitors. Four channels of the Main Control Room Intake Radiation- High are available and three are required to be OPERABLE to ensure that no single instrument failure can preclude MCR isolation and MCRBA system initiation. The Allowable Value was selected to ensure protection of the control room personnel.

The Main Control Room Intake Radiation - High Function is required to be OPERABLE in MODES 1, 2, 3, and 4, and during OPDRVs and movement of irradiated fuel in the reactor building to ensure the control room personnel are protected during a LOCA, fuel handling event and a vessel drain down event. During MODES 5 and 6 the probability of a LOCA or fuel damage is low, thus the Function is not required. In addition, the Functions are required to be OPERABLE during operations with a potential for draining the reactor vessel and movement of irradiated fuel assemblies in the reactor building because the capability of detecting radiation releases due to fuel failures (due to fuel uncover or dropped fuel assemblies) must be provided to ensure off-site dose limits are not exceeded.

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 can be rapidly isolated when a need for isolation is indicated. Note 2 has been provided to modify the ACTIONS related to isolation. A second Note (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 Function with one or more required isolation instrumentation channels inoperable, the affected instrument division must be placed in trip. Because of the diversity of sensors available to provide trip signals and the redundancy of the isolation design, an allowable out of service time of 12 hours is considered acceptable to permit restoration of any inoperable channel to OPERABLE status. However, this out of service time is only acceptable provided the associated Function still maintains isolation trip capability (refer to Required Actions B.1 Bases). If the inoperable channel cannot be restored to OPERABLE status within the allowable out of service time, the affected instrument division must be placed in trip. Placing the isolation division in trip would conservatively compensate for the inoperability and allow operation to continue. Alternately, if it is not desired to place the division in trip (e.g., as in the case where placing the division in trip would result in an isolation and reactor scram), Condition C must be entered and its Required Action taken. Most repairs are likely to be simple card or other electronic subassembly replacements that can be done on-line with the affected division of sensors in bypass. In such cases, restoration should be done as soon as practicable.

B.1

Required Action B.1 is intended to ensure that appropriate actions are taken if multiple, inoperable, untripped channels (i.e., three or more channels for most Function) for the same Function result in the Function not maintaining isolation trip capability. A Function is considered to be maintaining isolation trip 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 is isolated.

The Completion Time is intended to allow the operator time to evaluate and repair any discovered inoperabilities. The 1 hour Completion Time is acceptable because it minimizes risk while allowing time for restoration or tripping of channels.

C.1

Required Action C.1 directs entry into the appropriate Condition referenced in Table 3.3.6.1-1. 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. Each time an inoperable channel has not met any Required Action of Condition A or B, and the associated Completion Time has expired, Condition C will be entered for that channel and provides for transfer to the appropriate subsequent Condition.

D.1

If the channel is not restored to OPERABLE status or placed in trip, or if isolation 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. This is done by placing the plant in at least MODE 2 within 6 hours.

BASES

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.

E.1 and E.2

If the channel is not restored to OPERABLE status or placed in trip, or if isolation 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 plant must be placed in a MODE in which overall plant risk is minimized. This is accomplished by placing the plant in MODE 3 within 12 hours or remaining in MODE 4. 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.

Remaining in the Applicability of the LCO is acceptable because the plant risk in MODE 3 and MODE 4 is similar to or lower than the risk in MODE 5) and because the time spent in MODE 3 to perform the necessary repairs to restore the system to OPERABLE status will be short. Going to cold shutdown results in challenges to the shutdown heat removal systems and requires restarting the plant. However, voluntary entry into MODE 5 may be made, as it is also an acceptable low-risk state.

Alternately, the associated MSLs and RWCU/SDC lines, as applicable may be isolated (Required Action E.1), and if allowed (i.e., plant safety analysis allows operation with an MSL isolated), plant operation with the MSL isolated may continue. Isolating the affected MSL and RWCU/SDC lines, as applicable accomplishes the safety function of the inoperable channel(s). The Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

F.1

If the channel is not restored to OPERABLE status or placed in trip, or if isolation trip capability is not restored within the allowed Completion Time, plant operation may continue if the affected penetration flow path(s) is isolated. Isolating the affected penetration flow path(s) accomplishes the safety function of the inoperable channels.

G.1

If the channel is not restored to OPERABLE status or placed in trip, or if isolation 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 plant must be placed in a MODE in which overall plant risk is minimized. This is accomplished by placing the plant in MODE 3 within 12 hours or remaining in MODE 4. 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.

Remaining in the Applicability of the LCO is acceptable because the plant risk in MODE 3 and MODE 4 is similar to or lower than the risk in MODE 5) and because the time spent in MODE 3 to perform the necessary repairs to restore the system to OPERABLE status will be short. Going to cold shutdown results in challenges to the shutdown heat removal systems and requires restarting the plant. However, voluntary entry into MODE 5 may be made, as it is also an acceptable low-risk state.

H.1 and H.2

If the channel is not restored to OPERABLE status or placed in trip, or if isolation trip capability is not restored within the allowed Completion Time, during movement of irradiated fuel assemblies in the reactor building or during OPDRVs, action must be taken to immediately suspend activities that represent a potential for releasing radioactivity that might require isolation of the reactor building or refueling area, This places the unit in a condition that minimizes risk. If applicable, movement of irradiated fuel assemblies in the reactor building must be immediately suspended. Suspension of these activities shall not preclude completion of movement of a component to a safe position. Also, if applicable, actions must be initiated immediately to suspend OPDRVs to minimize the probability of a vessel drain down and subsequent potential for fission-product release. Actions must continue until the OPDRVs are suspended.

Required Action H.2.1 has been modified by a Note which states that LCO 3.0.3 does not apply. If moving irradiated fuel while in MODE 1, 2, 3,or 4, the fuel movement is independent of reactor operations. Therefore, inability to suspend movement of irradiated fuel assemblies would not be a sufficient reason to require a reactor shutdown.

Alternately, the associated pathways may be isolated (Required Action H.1).

BASES

I.1 and I.2

If the channel is not restored to OPERABLE status or placed in trip or if isolation trip capability is not restored within the allowed Completion Time, the control room must be isolated and the actions must be taken to place the Emergency Breathing Air System (EBAS) in operation. In this situation the initiation system is degraded so that the ability to isolate the MCR and start the EBAS system cannot be assured. Therefore, further actions must be performed to ensure the ability to maintain the MCR envelope function. Isolating the associated valves and starting the EBAS system performs the intended function of the instrumentation and allows operations to continue.

J.1.1, J.1.2, J.2.1, and J.2.2

If the channel is not restored to OPERABLE status or placed in trip or if isolation trip capability is not restored within the allowed Completion Time, the ability to isolate the MCR and start the EBAS system cannot be assured. Therefore, further actions must be performed to ensure the ability to maintain the MCR envelope. Isolating the associated valves and starting the EBAS system performs the intended function of the instrumentation and allows operations to continue.

Alternately, the activities may be suspended. Therefore, action must be taken to immediately suspend activities that represent a potential for releasing radioactivity that might require isolation of the reactor building or refueling area. This places the unit in a condition that minimizes risk. If applicable, movement of irradiated fuel assemblies in the reactor building must be immediately suspended. Suspension of these activities shall not preclude completion of movement of a component to a safe position. Also, if applicable, actions must be initiated immediately to suspend OPDRVs to minimize the probability of a vessel drain down and subsequent potential for fission product release. Actions must continue until the OPDRVs are suspended.

Required Action J.2.1 has been modified by a Note which states that LCO 3.0.3 does not apply. If moving irradiated fuel while in MODE 1, 2, 3,or 4, the fuel movement is independent of reactor operations. Therefore, inability to suspend movement of irradiated fuel assemblies would not be a sufficient reason to require a reactor shutdown.

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 3.3.6.1-1.

The Surveillances are modified by a Note to indicate that a 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 for up to 6 hours provided the associated Function maintains trip capability. Upon Completion of the Surveillance, or expiration of the 6 hour allowance, the channel must be returned to OPERABLE status or the applicable Condition entered and Required Actions taken. This Note is based on the [reliability analysis] assumption that 6 hours is the average time required to perform channel Surveillance. That analysis demonstrated that the 6 hour testing allowance does not significantly reduce the probability that the valves will isolate the penetrations when necessary.

SR 3.3.6.1.1

Performance of the CHANNEL CHECK once every [24] hours ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is a comparison of the parameter indicated on one channel to a similar parameter in other channels. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value. Significant deviations between the two instrument channels could be an indication of excessive instrument drift in one of the channels or even something more serious. A CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

Agreement criteria are determined by the 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. Thus, performance of the CHANNEL CHECK ensures that undetected outright channel failure is limited to [24] hours.

The CHANNEL CHECK supplements less formal, but more frequent checks of channel 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.

If the as-found setpoint is not within its required Allowable Value the plant specific setpoint methodology may be revised, as appropriate if the history and all other pertinent information indicates a need for the revision. The setpoint shall be left set consistent with the assumptions of the current plant-specific setpoint methodology.

The Surveillance Frequency is based on [reliability analysis].

SR 3.3.6.1.3

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 account for instrument drifts between successive calibrations. Measurement and setpoint error historical determinations must be performed consistent with the plant specific setpoint methodology. The channel shall be left calibrated consistent with the assumptions of the setpoint methodology.

If the as-found setpoint is not within its required Allowable Value the plant specific setpoint methodology may be revised, as appropriate, if the history and all other pertinent information indicates a need for the revision. The setpoint shall be left set consistent with the assumptions of the current plant-specific setpoint methodology.

The Surveillance Frequency is based upon 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 3.3.1.6.4

This SR ensures that the individual 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.

A Note to the Surveillance states that the radiation detectors may be

BASES

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.

ISOLATION SYSTEM RESPONSE TIME tests are conducted at a 24 month on a STAGGERED TEST BASIS. Therefore, staggered testing results in response time verification of these devices every 24 months. The 24 month test Frequency is consistent with the typical industry refueling cycle and is based upon plant operating experience, which shows that random failures of instrumentation components causing serious time degradation, but not channel failure, are infrequent occurrences.

REFERENCES

1. Chapter 6.
2. Chapter 15.

B 3.3 INSTRUMENTATION

B 3.3.6.2 Isolation Actuation

BASES

BACKGROUND

The digitally multiplexed isolation system utilizes a two-out-of-four trip initiation logic. Four separate instrument divisions are used to monitor the required parameters. Four separate divisions of trip logic are then used to perform the required trip determination. This occurs within the divisional Digital Trip Modules (DTMs). Each divisional DTM receives input from the instrumentation in that same division for each parameter monitored. For analog parameters the DTMs make the trip/no-trip decision by comparing a digitized analog value against a setpoint and initiating a trip condition for that parameter if the setpoint is exceeded. The output of each divisional DTM (a trip/no-trip condition) for each parameter is then routed to all four divisional Trip Logic Units (TLUs) such that each divisional TLU receives input from each of the four divisions of DTMs. Each DTM has a division-of-sensors bypass such that all instruments in that division can be bypassed in the isolation trip logic at the TLUs. In this condition each TLU would be making its trip decision on a two-out-of-three logic basis for each parameter. 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 parameter basis such that setpoint exceedence in two instrument divisions for the same parameter 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. Each TLU has a bypass switch so that they can be bypassed, only one at any one time, such that the isolation 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 isolation.

For main steam isolation valves (MSIVs) and main steam line (MSL) drains, a two-out-of-four trip in a TLU causes a trip in its corresponding Output Logic Unit (OLU). It is this trip that then initiates a main steam isolation. The overall arrangement of OLU outputs and load driver for MSIV and MSL drain isolation is such that a trip of any two of four TLUs (and associated OLUs) will cause the complete closure of all MSIVs and MSL drain valves.

The other isolations are done in the Emergency Core Cooling System (ECCS) SSLC and logic for the affected system. This logic will be the same as the ECCS logic in that it will use four divisions of sensors (with a division of sensors bypass switch) and two two-out-of-four trip decisions per division that each operates a LD. Although all four divisions contribute to the isolation decision, the LDs in question reside in the division in which the isolation valve is powered (usually Division 1 and Division 2). There is also (non isolation) logic in the same division to operate the valve normally (i.e., open it). These isolation LDs are wired in series such that each division must make a two-out-of-two decision (the single failure for isolation is the valve in the other division).

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

The isolation signals generated by the isolation instrumentation are implicitly assumed in the safety analyses of References 1 and 2 to initiate closure of valves to limit off-site doses.

The isolation signals generated by the reactor building and refueling area exhaust isolation instrumentation are implicitly assumed in the safety analyses to initiate closure of valves to limit off site doses.

The ability of EBAS to maintain the habitability of the MCR is explicitly assumed for certain accidents as discussed in the safety analyses. The isolation of the control room and the operation of EBAS ensures the radiation exposure of control room personnel, through the duration of any one of the postulated accidents, does not exceed the limits set by GDC 19 of 10 CFR 50, Appendix A.

Isolation actuation instrumentation satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

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

In general, the individual isolation actuation Functions are required to be OPERABLE in the MODES or other specified conditions when to support the isolation instrumentation required by LCO 3.3.6.1, "Isolation Instrumentation."

1. Main Steam Isolation Valves and Drains

The Main Steam Isolation Valves and Drains isolation actuation supports the following isolation instrumentation in LCO 3.3.6.1: Reactor Vessel Water Level - Low, Level 2; Reactor Vessel Water Level - Low, Level 1; Main Steam Line Pressure - Low; Main Steam Line Flow - High (Per Steam Line); Condenser Vacuum - Low; Main Steam Tunnel Ambient Temperature - High; and Main Steam Turbine Area Ambient Temperature

– High. [Three] channels per valve of Main Steam Isolation Valves and Drains isolation actuation are required to be OPERABLE ensure no single isolation actuation failure can preclude the isolation function. The Function is required to be OPERABLE in MODES 1, 2, 3, and 4.

2. Reactor Water Cleanup/Shutdown Cooling Lines

The Reactor Water Cleanup/Shutdown Cooling Lines isolation actuation channels supports 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 Subsystem Flow - High Functions. Four Reactor Water Cleanup/Shutdown Cooling Lines isolation actuation channels are required to be OPERABLE to ensure no single isolation actuation failure can preclude the isolation function. The Function is required to be OPERABLE in MODES 1, 2, 3, 4, 5 and 6.

3. Isolation Condenser

The Isolation Condenser isolation actuation channels supports the Reactor Vessel Water Level - Low, Level 2, Reactor Vessel Water Level - Low, Level 1, Isolation Condenser Train Steam Line Flow - High (Per Isolation Condenser, Isolation Condenser Train Condensate Line Flow – High (Per Isolation Condenser), and Isolation Condenser Train Pool Vent Discharge Radiation - High (Per Isolation Condenser) Functions. Four Isolation Condenser isolation actuation channels per train are required to be OPERABLE to ensure no single isolation actuation failure can preclude the isolation function. The Function is required to be OPERABLE in MODES 1, 2, 3, and 4.

4. Fission Product Sampling Lines

The Fission Product Sampling Lines isolation actuation channels supports the Reactor Vessel Water Level - Low, Level 2, Reactor Vessel Water Level - Low, Level 1, and Drywell Pressure Functions. Four Fission Product Sampling Lines isolation actuation channels are required to be OPERABLE to ensure no single isolation actuation failure can preclude the isolation function. The Function is required to be OPERABLE in MODES 1, 2, 3, and 4.

5. Drywell High Conductivity Waste Sump Drain Line

The Drywell High Conductivity Waste Sump Drain Line isolation actuation channels supports the Reactor Vessel Water Level - Low, Level 2, Reactor Vessel Water Level - Low, Level 1, and Drywell Pressure Functions. Four Drywell High Conductivity Waste Sump Drain Line isolation actuation channels are required to be OPERABLE to ensure no single isolation actuation failure can preclude the isolation function. The Function is required to be OPERABLE in MODES 1, 2, 3, and 4.

6. Drywell Low Conductivity Waste Sump Drain Line

The Drywell Low Conductivity Waste Sump Drain Line isolation actuation channels supports the Reactor Vessel Water Level - Low, Level 2, Reactor Vessel Water Level - Low, Level 1, and Drywell Pressure Functions. Four Drywell High Conductivity Waste Sump Drain Line isolation actuation channels are required to be OPERABLE to ensure no single isolation actuation failure can preclude the isolation function. The Function is required to be OPERABLE in MODES 1, 2, 3, and 4.

7. Containment Purge and Vent Valve isolation actuation

The Containment Purge and Vent Valve isolation actuation channels supports the Reactor Vessel Water Level - Low, Level 2, Reactor Vessel Water Level - Low, Level 1, Reactor Building HVAC Exhaust Radiation - High, Refueling Area Exhaust Radiation - High, and Drywell Pressure Functions. Four Containment Purge and Vent Valve isolation actuation channels are required to be OPERABLE to ensure no single isolation actuation failure can preclude the isolation function. The Function is required to be OPERABLE in MODES 1, 2, 3, and 4.

8. Reactor Component Cooling Water to the Drywell Air Coolers

The Reactor Component Cooling Water to the Drywell Air Coolers isolation actuation channels supports the Reactor Vessel Water Level - Low, Level 2, Reactor Vessel Water Level - Low, Level 1, and Drywell Pressure - High Functions. Four Reactor Component Cooling Water to the Drywell Air Coolers isolation actuation channels are required to be OPERABLE to ensure no single isolation actuation failure can preclude the isolation function. The Function is required to be OPERABLE in MODES 1, 2, 3, and 4.

9. Fuel and Auxiliary Pools Cooling System

The Fuel and Auxiliary Pools Cooling System isolation actuation channels supports the Reactor Vessel Water Level - Low, Level 2, Reactor Vessel Water Level - Low, Level 1, and Drywell Pressure - High Functions. Four Fuel and Auxiliary Pools Cooling System isolation actuation channels are required to be OPERABLE to ensure no single isolation actuation failure can preclude the isolation function. The Function is required to be OPERABLE in MODES 1, 2, 3, and 4.

10. Reactor Building HVAC Exhaust

Reactor Building HVAC Exhaust isolation actuation channels supports the Reactor Vessel Water Level - Low, Level 2, Reactor Vessel Water Level - Low, Level 1, Drywell Pressure - High, Reactor Building HVAC Exhaust Radiation - High, and Refueling Area Exhaust Radiation - High. Four Reactor Building HVAC Exhaust isolation actuation channels are required to be OPERABLE to ensure no single isolation actuation failure can preclude the isolation function. The Function is required to be OPERABLE in MODES 1, 2, 3, and 4, during operations with a potential for draining the reactor vessel, and during movement of irradiated fuel in the reactor building.

11. Main Control Room

Main Control Room Isolation actuation channels supports the Main Control Room Intake Radiation - High Function. Four Main Control Room isolation actuation channels are required to be OPERABLE to ensure no single isolation actuation failure can preclude the isolation and EBAS actuation functions. The Function is required to be OPERABLE in MODES 1, 2, 3, and 4, during operations with a potential for draining the reactor vessel, and during movement of irradiated fuel in the reactor building.

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 can be rapidly isolated when a need for isolation is indicated. Note 2 have been provided to modify the ACTIONS related to isolation. A second Note (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 Function with one or more required isolation instrumentation channels inoperable, the affected [channel] must be placed in trip. Because of the redundancy of the isolation design, an allowable out of service time of 12 hours is considered acceptable to permit restoration of any inoperable channel to OPERABLE status. However, this out of service time is only acceptable provided the associated Function still maintains isolation trip capability (refer to Required Actions B.1 Bases). If the inoperable channel cannot be restored to OPERABLE status within the allowable out of service time, the affected channel must be placed in trip. Placing the channel in trip would conservatively compensate for the inoperability and allow operation to continue. Alternately, if it is not desired to place the division in trip (e.g., as in the case where it would result in an isolation and reactor scram), Condition C must be entered and its Required Action taken. Most repairs are likely to be simple card or other electronic subassembly replacements that can be done on-line with the affected division of sensors in bypass. In such cases, restoration should be done as soon as practicable.

B.1

Required Action B.1 is intended to ensure that appropriate actions are taken if multiple, inoperable, untripped channels (i.e., three or more channels for most Function) for the same Function result in the Function not maintaining isolation trip capability. A Function is considered to be maintaining isolation trip 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 is isolated.

The Completion Time is intended to allow the operator time to evaluate and repair any discovered inoperabilities. The 1 hour Completion Time is acceptable because it minimizes risk while allowing time for restoration or tripping of channels.

C.1

Required Action C.1 directs entry into the appropriate Condition referenced in Table 3.3.6.1-1. 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. Each time an inoperable channel has not met any Required Action of Condition A or B, and the associated Completion Time has expired, Condition C will be entered for that channel and provides for transfer to the appropriate subsequent Condition.

D.1

If the channel is not restored to OPERABLE status or placed in trip, or if isolation trip capability is not restored within the allowed Completion Time, plant operation may continue if the affected penetration flow path(s) is isolated. Isolating the affected penetration flow path(s) accomplishes the safety function of the inoperable channels.

E.1

If the channel is not restored to OPERABLE status or placed in trip, or if isolation 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 plant must be placed in a MODE in which overall plant risk is minimized. This is accomplished by placing the plant in MODE 3 within 12 hours or remaining in MODE 4. 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.

Remaining in the Applicability of the LCO is acceptable because the plant risk in MODE 3 and MODE 4 is similar to or lower than the risk in MODE 5) and because the time spent in MODE 3 to perform the necessary repairs to restore the system to OPERABLE status will be short. Going to cold shutdown results in challenges to the shutdown heat removal systems and requires restarting the plant. However, voluntary entry into MODE 5 may be made, as it is also an acceptable low-risk state.

F.1 and F.2

If the channel is not restored to OPERABLE status or placed in trip, or if isolation 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 plant must be placed in a MODE in which overall plant risk is minimized. This is accomplished by placing the plant in MODE 3 within 12 hours or remaining in MODE 4. 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.

Remaining in the Applicability of the LCO is acceptable because the plant risk in MODE 3 and MODE 4 is similar to or lower than the risk in MODE 5) and because the time spent in MODE 3 to perform the necessary repairs to restore the system to OPERABLE status will be short. Going to cold shutdown results in challenges to the shutdown heat removal systems and requires restarting the plant. However, voluntary entry into MODE 5 may be made, as it is also an acceptable low-risk state.

Alternately, the associated [MSLs and RWCU/SDC lines], as applicable may be isolated (Required Action F.1), and if allowed (i.e., plant safety analysis allows operation with an MSL isolated), plant operation with the MSL isolated may continue. Isolating the affected MSL and RWCU/SDC lines, as applicable accomplishes the safety function of the inoperable channel(s). The Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

<u>G.1, G.2.1, and G.2.2</u>

If the channel is not restored to OPERABLE status or placed in trip, or if isolation trip capability is not restored within the allowed Completion Time, during movement of irradiated fuel assemblies in the reactor building or during OPDRVs, action must be taken to immediately suspend activities that represent a potential for releasing radioactivity that might require isolation of the reactor building or refueling area, This places the unit in a condition that minimizes risk. If applicable, movement of irradiated fuel assemblies in the reactor building must be immediately suspended. Suspension of these activities shall not preclude completion of movement of a component to a safe position. Also, if applicable, actions must be initiated immediately to suspend OPDRVs to minimize the probability of a vessel drain down and subsequent potential for fission-product release. Actions must continue until the OPDRVs are suspended.

Required Action G.2.1 has been modified by a Note which states that LCO 3.0.3 does not apply. If moving irradiated fuel while in MODE 1, 2, 3,or 4, the fuel movement is independent of reactor operations.

Therefore, inability to suspend movement of irradiated fuel assemblies would not be a sufficient reason to require a reactor shutdown.

Alternately, the associated pathways may be isolated (Required Action G.1).

H.1 and H.2

If the channel is not restored to OPERABLE status or placed in trip or if isolation trip capability is not restored within the allowed Completion Time, the control room must be isolated and the actions must be taken to place the Emergency Breathing Air System (EBAS) in operation. In this situation the initiation system is degraded so that the ability to isolate the MCR and start the EBAS system cannot be assured. Therefore, further actions must be performed to ensure the ability to maintain the MCR envelope function. Isolating the associated valves and starting the EBAS system performs the intended function of the instrumentation and allows operations to continue.

I.1.1, I.1.2, I.2.1, and I.2.2

If the channel is not restored to OPERABLE status or placed in trip or if isolation trip capability is not restored within the allowed Completion Time, the ability to isolate the MCR and start the EBAS system cannot be assured. Therefore, further actions must be performed to ensure the ability to maintain the MCR envelope. Isolating the associated valves and starting the EBAS system performs the intended function of the instrumentation and allows operations to continue.

Alternately, the activities may be suspended. Therefore, action must be taken to immediately suspend activities that represent a potential for releasing radioactivity that might require isolation of the reactor building or refueling area. This places the unit in a condition that minimizes risk. If applicable, movement of irradiated fuel assemblies in the reactor building must be immediately suspended. Suspension of these activities shall not preclude completion of movement of a component to a safe position. Also, if applicable, actions must be initiated immediately to suspend OPDRVs to minimize the probability of a vessel drain down and subsequent potential for fission product release. Actions must continue until the OPDRVs are suspended.

Required Action I.2.1 has been modified by a Note which states that LCO 3.0.3 does not apply. If moving irradiated fuel while in MODE 1, 2, 3, or 4, the fuel movement is independent of reactor operations.

BASES

Therefore, inability to suspend movement of irradiated fuel assemblies would not be a sufficient reason to require a reactor shutdown.

J.1 and J.2

If the channel is not restored to OPERABLE status or placed in trip within the allowed Completion Time, the associated penetration flow path should be closed. However, if the shutdown cooling function is needed to provide core cooling, these Required Actions allow the penetration flow path to remain unisolated provided action is immediately initiated to restore the channel to OPERABLE status or to isolate the Reactor Water Cleanup/ Shutdown Cooling (i.e., provide alternate decay heat removal capabilities so the penetration flow path can be isolated). ACTIONS must continue until the channel is restored to OPERABLE status or the Reactor Water Cleanup Shutdown Cooling System is isolated.

SURVEILLANCE REQUIREMENTS

The Surveillances are modified by a Note to indicate that a 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 for up to 6 hours provided the associated Function maintains trip capability. Upon Completion of the Surveillance, or expiration of the 6 hour allowance, the channel must be returned to OPERABLE status or the applicable Condition entered and Required Actions taken. This Note is based on the reliability analysis (Refs. 3 and 4) assumption that 6 hours is the average time required to perform channel Surveillance. That analysis demonstrated that the 6 hour testing allowance does not significantly reduce the probability that the isolation will occur when necessary.

SR 3.3.6.2.1

The LOGIC SYSTEM FUNCTIONAL TEST demonstrates the OPERABILITY of the required isolation logic for a specific channel. The Surveillance Frequency at the 24 MONTH for SR 3.3.6.2.6 was developed considering it is prudent that the Surveillance be performed only during a plant outage.

This is due to the plant conditions needed to perform the surveillance and the potential for unplanned transients if the surveillance is performed with the reactor at power. Operating experience has shown these components usually pass the Surveillance when performed at the 24 month Frequency.

BASES

[SR 3.3.6.2.2

This SR ensures that the individual 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 closure times to obtain the ISOLATION SYSTEM RESPONSE TIME. ISOLATION SYSTEM RESPONSE TIME acceptance criteria are included in Reference [2].

ISOLATION SYSTEM RESPONSE TIME may be verified by actual response time measurements in any series of sequential, overlapping, or total channel measurements.

ISOLATION SYSTEM RESPONSE TIME tests are conducted on an 24 month STAGGERED TEST BASIS. The 24 month test Frequency is consistent with the typical industry refueling cycle and is based upon plant operating experience that shows that random failures of instrumentation components causing serious response time degradation, but not channel failure, are infrequent.]

REFERENCES

1. Chapter 6.
2. Chapter 15.

B 3.4 REACTOR COOLANT SYSTEM (RCS)

B 3.4.1 Safety/Relief Valves (S/RVs)

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 S/RVs 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 S/RVs are located on the main steam lines between the reactor vessel and the first isolation valve within the drywell. Ten S/RVs discharge steam through a discharge line directly to a point below the minimum water level in the suppression pool. The remaining eight S/RVs discharge steam, through individual discharge lines, to one of two common headers with rupture discs that discharge into the drywell. Additionally, each common header also has one discharge line to a point below the minimum water level in the suppression pool. The S/RVs are capable of being actuated in one or both of two modes: the safety mode and the Automatic Depressurization System (ADS) power actuated mode. All eighteen S/RVs are capable of functioning in the safety mode (or spring actuated mode of operation). 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 plus the weight of the disk. Ten of the S/RVs are also capable of functioning in the ADS mode. In the ADS mode, a pneumatic piston or cylinder and mechanical linkage assembly are used to open the valve by overcoming the spring force, even with the valve inlet pressure equal to zero psig. The pneumatic operator is arranged so that its malfunction will not prevent the valve disk from lifting if steam inlet pressure reaches the spring lift set pressures. The ten S/RVs that provide the ADS function can be opened manually or automatically as part of the Automatic Depressurization System specified in LCO 3.5.1, “ECCS–Operating.” The instrumentation associated with the relief valve function of the ADS is discussed in the Bases for LCO 3.3.5.1, “Emergency Core Cooling System (ECCS) Instrumentation.”

BASES

APPLICABLE SAFETY ANALYSES

The overpressure protection system must accommodate the most severe pressure transient. Evaluations have determined that the most severe pressure transient is the [closure of all main steamline isolation valves (MSIVs) followed by reactor scram on high neutron flux (i.e., failure of the direct scram associated with MSIV position)] (Ref. 2). The analysis results demonstrate that the design S/RV capacity 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). [Five] S/RVs are required to be OPERABLE in the safety mode to meet single failure considerations. This LCO helps to ensure that the acceptance limit of 9.48 MPaG (1375 psig) is met during the design basis event.

The additional events discussed in Reference 3 are not expected to actuate the S/RVs. From an overpressure standpoint, these events are bounded by the [MSIV closure with flux scram] event described above.

Safety/relief valves satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

[Eighteen] S/RVs are required to be OPERABLE in the safety mode. The requirements of this LCO are applicable only to the capability of the S/RVs to mechanically open to relieve excess pressure. The results in Reference 2 show that [eighteen] S/RVs are required OPERABLE to meet the minimum requirements for Anticipated Transients Without Scram (ATWS). Additionally, the results in Reference 2 show that with a minimum of [four] S/RVs in the safety mode OPERABLE, with setpoints in a distribution equivalent to, or conservative with respect to, the minimum requirements of SR 3.4.1.1, the ASME Code limit of 9.48 MPaG (1375 psig) is not exceeded. Therefore, [eighteen] S/RVs are required to be OPERABLE in the safety mode for an ATWS event, and [Five] S/RVs in the safety mode are required to be OPERABLE to satisfy the design basis overpressure event and provide for single failure criterion.

The S/RV 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 are based on these setpoints, but also include the additional uncertainties of ± 1% of the nominal setpoint to account for potential setpoint drift to provide an additional degree of conservatism.

BASES

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 S/RVs must be OPERABLE because there may be considerable energy in the reactor core and the limiting design basis transients are assumed to occur. The S/RVs may be required to provide pressure relief to discharge energy from the core until such time that the Gravity-Driven Cooling System (GDCS) is capable of dissipating the heat.

In MODE 5, decay heat is low enough for the GDCS to provide adequate cooling, and reactor pressure is low enough that the overpressure limit cannot 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. The S/RV function is not needed during these conditions.

ACTIONS

A.1

With the safety function of one S/RV inoperable, the remaining operable S/RVs are capable of providing the necessary overpressure protection. However, the overall reliability of the pressure relief system is reduced because additional failures in the remaining OPERABLE S/RVs could result in failure to adequately relieve pressure during a limiting event. For this reason, continued operation is permitted for a limited time only.

The 14-day Completion Time to restore the inoperable S/RVs to OPERABLE status is based on the relief capability of the remaining S/RVs, the low probability of an event requiring S/RV actuation, and a reasonable time to complete the Required Action.

B.1 and B2

With less than the minimum number of S/RVs OPERABLE, a transient may result in the violation of the ASME Code limit on reactor pressure. If the inoperable S/RV cannot be restored to OPERABLE status within the associated Completion Time of Required Action A.1 or if [fourteen] or more required S/RVs are inoperable, 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 operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.4.1.1

This Surveillance demonstrates that the S/RVs will open at the pressures assumed in the safety analysis of Reference 2. The demonstration of the S/RV safety function lift settings is a bench test and must be performed during shutdown. The lift setting pressure shall correspond to ambient conditions of the valves at nominal operating temperatures and pressures. The S/RV setpoint is ± [3]% for OPERABILITY; however the valves are reset to ± [1]% during the Surveillance to allow for drift.

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.

3. Chapter 15.

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 or bolted.

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).

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.

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.

BASES

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 [19 L/min (5 gpm)] limit is a small fraction of the calculated flow from a critical crack in the primary system piping. Crack behavior from experimental programs (Refs. 4 and 5) shows leak rates of hundreds of Liters per minute (hundreds of gpm) will precede crack instability (Ref. 6).

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.

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.

BASES

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 identify the source, determine the significance of the leak, and 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.

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.

BASES

SURVEILLANCE REQUIREMENTS	<u>SR 3.4.2.1</u> 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 7. 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. 8).
REFERENCES	1. 10 CFR 50.2. 2. 10 CFR 50.55a(c). 3. 10 CFR 50, Appendix A, Section V, GDC 55. 4. GEAP-5620, April 1968. 5. NUREG-76/067, October 1975. 6. Section 5.2.5. 7. Regulatory Guide 1.45. 8. 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 50 (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 50 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 main steam line break (MSLB) outside containment. No fuel damage is postulated in the MSLB accident, and the release of radioactive material to the environment is assumed to end when the main steam isolation valves (MSIVs) close completely.

This MSLB release forms the basis for determining 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 a MSLB outside containment during steady state operations, will not exceed the dose guidelines of Regulatory Guide 1.183 (Ref. 3).

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,

BASES

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 for the MSLB is not exceeded, so any release of radioactivity to the environment during an MSLB is less than the Regulatory Guide 1.183 limits.

APPLICABILITY

In MODE 1, and MODES 2, 3, and 4 with any main steam line not isolated, 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 an MSLB outside of primary containment.

In MODES 2, 3, and 4, with the MSIVs closed, such limits do not apply because an escape path does not exist. 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.

B.1 and B.2

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 and all the main steam lines must be isolated within 12 hours. Isolating the main steam lines precludes the possibility of releasing radioactive material to

BASES

the environment more than the requirements of Regulatory Guide 1.183 during a postulated MSLB accident.

The Completion Time of once every 4 hours is the time needed to take and analyze a sample. The 12-hour Completion Time is reasonable, based on operating experience, to isolate the main steam lines 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 50.34.

2. Chapter 15.

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.

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 CFR50, 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 (RTNDT) 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

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. The ASME Code, Section XI, Appendix E (Ref. 6), provides a recommended methodology for evaluating an operating event that causes an excursion outside the limits.

APPLICABLE SAFETY ANALYSES

The P/T limits are not derived from Design Basis Accident (DBA) analyses. They are prescribed during normal operation to avoid encountering pressure, temperature, and temperature rate-of-change conditions that might cause undetected flaws to propagate and cause non-ductile failure of the RCPB, a condition that is unanalyzed. Reference 7 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:

a. RCS pressure, temperature, and heatup or cooldown rate are within the limits specified in the PTLR;

b. RCS pressure and temperature are within the criticality limits specified in the PTLR, prior to achieving criticality; and

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.

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.

BASES

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.

ASME Section XI, Appendix E (Ref. 6), may be used to support the evaluation. However, its use is restricted to evaluation of the vessel beltline.

The 72-hour Completion Time is reasonable to accomplish the evaluation. The evaluation for a mild violation is possible within this time, but more severe violations may require special, event-specific stress analyses or inspections. A favorable evaluation must be completed 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.

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

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 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. ASME Section XI, Appendix E (Ref. 6), may be used to support the evaluation; however, its use is restricted to evaluation of the beltline.

SURVEILLANCE REQUIREMENTS

SR 3.4.4.1

Verification that operation is within PTLR limits is required every 30 minutes when RCS pressure and temperature conditions are undergoing planned changes. This Frequency is considered reasonable in view of the control room indication available to monitor RCS status. Also, since temperature rate-of-change limits are specified in hourly increments, 30 minutes permits assessment and correction 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.

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

BASES

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.

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 185-94, July 1994.
4. 10 CFR 50, Appendix H.
5. Regulatory Guide 1.99, Revision 2, May 1988.
6. ASME, *Boiler and Pressure Vessel Code*, Section XI, Appendix E.
7. NEDO-21778-A, December 1978.

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 2 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 5.2.
2. Chapter 15.

B 3.4 REACTOR COOLANT SYSTEM (RCS)

B 3.4.6 Isolation Condenser System (ICS)

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 (S/RV) operation, conserve RPV water level, and provide core cooling. The ICS (Ref. 1) is a passive high pressure system comprised of four physically, mechanically, and electrically independent natural circulation trains. Each ICS train consists of an isolation condenser (IC) unit and associated piping and valves. Each IC is located above and outside the drywell in a separate sub-compartment of the ICS/Passive Containment Cooling System (ICS/PCCS) pools. The IC steam side is connected to the reactor pressure vessel via two normally open series isolation valves. The IC condensate side is connected to the RCS loops via two normally open series isolation valves and two normally closed parallel return valves. The closed condensate return valves allow the isolation condenser and drain piping to fill with condensate, which is maintained at a subcooled temperature by the ICS/PCCS pool water during normal reactor operation. Upon initiation, the ICS condensate side valves are opened draining the IC and condensate lines to the RPV. High pressure steam from the RPV is then fed through the ICS steam supply line to the IC, where the steam transfers heat to the water in the ICS/PCCS pool, which is vented to the atmosphere. The steam in the IC condenses and drains back to the RPV via the condensate line. Each IC unit is designed for 33.75 MWt capacity, and any three of the four IC loops have the capability (90 MWt) to limit RPV temperature and pressure to acceptable ranges and provide decay heat cooling.
APPLICABLE SAFETY ANALYSES	The ICS is assumed to function following an RPV isolation or low water level (Level 2) event (Ref. 2). Although not a safety function, operation of three of the four ICS loops after an isolation or low water level event will limit reactor temperature and pressure to acceptable ranges such that automatic reactor depressurization or S/RV actuation will not occur as a result of a reactor pressure increase or coolant inventory loss. The ICS functions to reduce RPV pressure, conserve RPV water level, and provide removal of excess sensible and core decay heat following isolation events in MODES 1, 2, 3, and 4.

BASES

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

LCO

The LCO requires [four] trains of ICS be OPERABLE. Following a sudden reactor isolation or low water level (Level 2) event the ICS is required to be OPERABLE to: (1) limit reactor pressure and temperature within acceptable limits such that automatic reactor depressurization and S/RV actuation does not occur; and (2) remove excess sensible heat and core decay heat from the reactor.

An OPERABLE ICS requires the condensate return valves to open in response to closure of the Main Steam Isolation Valves, reactor low water level (Level 2), or high RPV pressure. This assumption is within the assumptions of the applicable analyses (Ref. 2).

APPLICABILITY

The ICS is required to be OPERABLE in MODES 1 and 2, and MODES 3 and 4 when < 12 hours since reactor was critical, to remove reactor decay heat following reactor shutdown and isolation. In addition, in MODES 1 and 2 the ICS is required to be OPERABLE to prevent unnecessary automatic reactor depressurization or S/RV actuation following RPV isolation or low water level events.

ACTIONS

<u>A.1</u>

If one of the four ICS trains is inoperable the remaining three trains have adequate capacity to meet the assumptions of the design basis transient analysis events (Ref. 2). However, the overall reliability is reduced because a single failure in one of the OPERABLE trains could result in reduced pressure attenuating or cooling capability. Therefore, the inoperable ICS loop should be restored to OPERABLE status within 14 days.

The Completion Time of 14 days is acceptable because in this condition the remaining three ICS trains are sufficient to meet the assumptions described in Reference 2.

B.1

If two of the four ICS trains are inoperable, one IC train must be restored to OPERABLE status within 72 hours. In this condition the ICS may not have sufficient capacity to attenuate RPV pressure to acceptable ranges that would preclude the use of automatic depressurization, or to provide adequate core cooling.

The Completion Time of 72 hours is reasonable based on the availability of alternate pressure and temperature control functions, the low probability of an event occurring that would require the ICS, and operating experience.

C.1

If three of the four ICS trains are inoperable, one IC train must be restored to OPERABLE status within 1 hour. In this condition the ICS does not have sufficient capacity to attenuate RPV pressure to acceptable ranges that would preclude the use of automatic depressurization, or to provide adequate core cooling.

The Completion Time of 1 hour is reasonable based on the availability of alternate pressure and temperature control functions, the low probability of an event occurring that would require the ICS, and operating experience.

D.1

If an inoperable ICS train cannot be restored to OPERABLE status within the associated Completion Times of Conditions A, B, or C, or four ICS trains are inoperable, 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 operating experience, to reach the required unit conditions from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.4.6.1

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. Because of the simplicity of the ICS design and the requirement that block valves for the ICS/PCCS pool must be locked open, this SR will require periodic verification of very few valves.

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 3.4.6.2

This SR requires periodic verification that the ICS/PCCS pool ICS subcompartment manual isolation valves are locked open. This SR is necessary to ensure that the required volume of water is available to each condenser.

The 24 month Frequency for this SR is based on engineering judgment and is acceptable because the manual isolation valves between the ICS/PCCS pool and the ICS sub-compartments are locked open and maintained in their correct position under administrative controls.

SR 3.4.6.3

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. This test overlaps Surveillance testing required in the instrumentation section of the Technical Specifications and is intended to provide complete testing of the assumed safety 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. From past operating

BASES

experience it is believed that these components will pass the SR when performed once per 24 months (i.e., the refueling interval).

REFERENCES

1. Chapter 5.
2. Chapter 15.

B 3.4 REACTOR COOLANT SYSTEM (RCS)

B 3.4.7 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, conserve RPV water level, and provide core cooling (Ref. 1). A description of the ICS is provided in the Bases for LCO 3.4.6, “Isolation Condenser System (ICS).” 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 System (RWCU/SDC) for decay heat removal.

RWCU/SDC consists to two [100% capacity] independent and redundant trains powered from separate electrical divisions that can be powered from either offsite power or either of the station diesel generators. If both loops are available, RWCU/SDC has the capacity to perform the decay heat removal function [and reduce reactor temperature] after the reactor has been shutdown for approximately [2] hours. If only one loop is available, RWCU/SDC has the capacity to perform the decay heat removal function after the reactor has been shutdown for approximately [12] hours. 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, 5, and 6. When the ICS/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. It is important to note that during decay heat removal using the ICS, a MODE change (MODE 5 to MODE 4) will occur due to the heat up of the RCS.

Use of the ICS as an emergency backup for decay heat removal in MODE 6 requires the reactor vessel head to be in place [with a sufficient number of head bolts head bolts tensioned to support the anticipated

BASES

	increase in reactor pressure when using the ICS for decay heat removal.] Once the reactor vessel head is removed, loss of the normal decay heat removal method could result in boiling in the vessel. Water in the GDCS pools, required to be available in LCO 3.5.2, “ECCS – Shutdown,” is one potential source of reactor coolant inventory if this is the only method of decay heat removal that is available.
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. Decay heat removal is, however, an important safety function that must be accomplished or core damage could result. ICS - Shutdown satisfies Criterion 4 of 10 CFR 50.36(c)(2)(ii).
LCO	This LCO requires that [two] trains of ICS be OPERABLE when shutdown to provide a backup method for decay heat removal. Although various methods of active decay heat removal using feed and bleed may be available, this LCO is intended to ensure that at least one highly reliable and [passive] alternative to RWCU/SDC for decay heat removal is available when in MODES 3, 4, 5 and when in MODE 6 until reactor pressure vessel head is removed.
APPLICABILITY	This LCO requires that [two] trains of ICS be OPERABLE in MODES 3 and 4 when > [12] hours since reactor was critical, in MODE 5, and in MODE 6 when the reactor vessel head is in place.
ACTIONS	<u>A.1</u> If one [or both] of the required ICS train[s 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 to ensure that a minimum of two methods capable of decay heat removal is available. The Completion Time of 4 hours recognizes the need to maintain redundant decay heat removal capability.

BASES

B.1

If redundant decay heat removal capability is not available, action must be initiated immediately to restore Reactor Building to OPERABLE status as described in the Bases for LCO 3.6.3.1, “Reactor Building.” This action is needed to establish appropriate compensatory measures for a loss of decay heat removal.

SURVEILLANCE REQUIREMENTS

SR 3.4.7.1

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 correct, since these were verified to be in the correct position upon locking, sealing, or securing. Because of the simplicity of the ICS design and the requirement that block valves for the ICS/PCCS pool must be locked open, this SR will require periodic verification of very few valves.

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 3.4.7.2

This SR requires periodic verification that pool subcompartment manual isolation valves are locked open. This SR is needed to ensure that the required volume of water is available to each condenser.

The 24 month Frequency for this SR is based on engineering judgment and is acceptable because the equalizing valves between ICS/PCCS pool sub-compartments are locked open and under administrative controls.

BASES

SR 3.4.7.3

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. This test overlaps Surveillance testing required in the instrumentation section of the Technical Specifications and is intended to provide complete testing of the assumed safety 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. From past operating experience it is believed that these components will pass the SR when performed once per 24 months (i.e., the refueling interval).

REFERENCES

1. Chapter 7.
2. Chapter 15.

B 3.5 EMERGENCY CORE COOLING SYSTEM (ECCS)

B 3.5.1 ECCS - Operating

BASES

BACKGROUND

The ECCS function is provided by the combination of the Gravity-Driven Cooling System (GDCS) and the Automatic Depressurization System (ADS). 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 four trains that are physically and mechanically independent with each of the four trains supported by a separate electrical division. Each of the four GDCS trains includes three subsystems: a GDCS short-term cooling (injection) subsystem; a GDCS long-term cooling (equalizing) subsystem; and, a GDCS deluge subsystem. Three GDCS pools, located within the drywell at an elevation above the reactor core, support all three subsystems for the four GDCS trains. The three GDCS pools are maintained with a sufficient volume of water to flood lower drywell and the reactor to a level [approximately 1 meter] above the core during a LOCA.

The four GDCS short-term cooling (GDCS injection) trains will refill the RPV following a LOCA after the RPV is depressurized. One of the GDCS pools is used to support two GDCS injection trains with the other two GDCS pools each supporting one of the remaining GDCS injection trains. Each GDCS injection train connects to the associated GDCS pool with a single pipe that includes a block valve at the GDCS pool. After entering the drywell annulus region, each GDCS injection train branches into two secondary lines. The eight GDCS injection secondary lines each include a check valve that prevents flow out of the RPV, a squib-actuated injection valve, and a block valve near the RPV. Each GDCS injection secondary line provides coolant to the annulus region of the reactor via an RPV nozzle located approximately [3] meters above the top of active fuel (TAF).

The four GDCS long-term cooling (GDCS equalizing) trains provide long term post-LOCA water makeup by connecting the annulus region of the reactor to the suppression pool. The suppression pool is located in the drywell slightly above the level of the core. Each GDCS equalizing train includes a block valve at the suppression pool, a check valve that prevents flow out of the RPV, a squib-actuated equalizing valve, and a block valve at the RPV. The four RPV nozzles used for the GDCS equalizing trains are located approximately [1] meter above TAF.

The four GDCS deluge trains may be used to dump any water remaining in the GDCS pools to the lower drywell in the event of a severe accident. The GDCS deluge trains provide a flow path from the GDCS pools via branch lies just downstream of the GDCS pool block valve of the associated GDCS injection train. Each of the four GDCS deluge trains branches into three lines, each branch line is equipped with a squib-actuated valve and a deluge line tailpipe located in the upper drywell. [The GDCS deluge trains are not required to satisfy the assumptions in any accident analysis. Therefore, OPERABILITY of the GDCS deluge subsystems is not required by Technical Specifications and is addressed in licensee controlled documents.]

The ADS (Ref.2) is an integral part of the ECCS because GDCS flow to the RPV requires that the RPV to be at a very low pressure. Therefore, the ADS is designed to depressurize the RPV following indication of a LOCA. [Although ADS is needed only for small-break LOCAs that do not depressurize the RPV, ADS is actuated every time the ECCS is actuated.]

The ADS consists of [ten] of the [eighteen] safety/relief valves (S/RVs) that have been configured to function as ADS valves and [eight] squib-actuated depressurization valves (DPVs). The ten dual function S/RVs are pneumatically actuated using energy stored in a nitrogen accumulator when functioning as ADS valves. Actuation is initiated by any of three solenoid-operated pilot valves powered by 250 VDC. Two of the solenoid-operated pilot valves are actuated by the Safety System Logic and Control (SSLC) logic and the third solenoid is actuated by the Diverse Protection System (DPS). [The DPS is not required to satisfy the assumptions in any accident analysis. Therefore, actuation of ADS using the DPS solenoids is not required by Technical Specifications and is addressed in licensee controlled documents.]

The initiation signal for ADS is designed to prevent inadvertent initiation. ADS actuates following [a RPV low water level (Level 1.5) signal confirmed by either high drywell pressure or a 15 minute time delay.] On receipt of the Level 1.5 initiation signal, the [ten] S/RVs designated as ADS valves and [eight] DPVs open in a pre-set timed sequence to depressurize the RPV.

The initiation signals for both the GDCS injection and GDCS equalizing subsystems are the same as used for ADS described above. Receipt of the GDCS initiation signal starts two sets of timers. Two [150] second timers actuate the squib valves in the secondary lines of the GDCS short-term cooling (GDCS injection) trains after allowing time for the ADS system to depressurize the RPV. Two [30] minute timers create a permissive signal that, in combination with [RPV water level below Level 0.5 (1 meter above TAF)], will actuate the squib valves in the GDCS long-term cooling (GDCS equalizing) trains. The initiation signal for the GDCS deluge subsystems is high temperature in the lower drywell floor area, which will actuate the squib valves in the GDCS deluge branch lines.

All ECCS subsystems are designed to ensure that no single active component failure will cause inadvertent initiation of ECCS or prevent automatic initiation and successful operation of the minimum required ECCS subsystems.

APPLICABLE SAFETY ANALYSES

ECCS performance is evaluated for the entire spectrum of break sizes for postulated LOCAs. The accidents for which ECCS operation is required are presented in Reference 3. The required ECCS analyses and assumptions are defined in 10 CFR 50 (Ref. 4), and the results of these analyses are described in Reference 3.

This LCO ensures that the following acceptance criteria for the ECCS, established by 10 CFR 50.46 (Ref. 5), will be met following a LOCA assuming the worst-case single active component failure in the ECCS:

a. Maximum fuel element cladding temperature is ≤ 1200°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.

The ADS and GDCS systems are designed with a large degree of redundancy and flexibility. 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 single failures are discussed in Reference 3.

For GDCS, Reference 3 indicates that [5] of the [8] GDCS injection secondary lines (i.e., [4] GDCS injection trains) and [1] of the [4] GDCS equalizing trains are needed to provide short-term and long-term core cooling following a LOCA. [A LOCA initiated by a break in one of the [8] GDCS injection secondary lines is assumed to disable the injection capability of both GDCS injection secondary lines in the GDCS injection train.] [The GDCS deluge trains are not required to satisfy the assumptions in any accident analysis.]

For ADS to support GDCS injection following a small break LOCA, Reference 3 indicates that depressurization requires a minimum of [6] of the [8] DPVs if all [10] of the ADS designated S/RVs function as required. If all [8] DPVs function as required, required depressurization will occur despite failure of multiple ADS designated S/RVs. [A single DPV is equivalent to approximately 3½ S/RVs in capacity.]

For ADS to support GDCS equalization following a [small break] LOCA, Reference 3 indicates that depressurization requires a minimum of [7] of the [8] DPVs if all [10] of the ADS designated S/RVs function as required. If all [8] DPVs function as required, required depressurization will occur despite failure of multiple ADS designated S/RVs.

The ECCS satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

This LCO for ECCS requires the OPERABILITY of each of the following:

a. [Four] trains of GDCS short-term cooling (injection) subsystem (i.e., [eight] GDCS injection secondary lines);
b. [Three] trains of the GDCS long-term cooling (equalizing) subsystem;
c. The ADS function of [ten] S/RVs; and
d. [Eight] Depressurization Valves (DPVs).

The LCO requirement for [eight] GDCS injection secondary lines satisfies the assumptions in Reference 3 for a LOCA initiated by a break in one of the GDCS injection secondary lines [that disables two secondary lines] and a single random failure that results in the failure of a third GDCS injection secondary line. In this scenario, the [5] remaining GDCS injection secondary lines are sufficient to satisfy accident analysis assumptions in Reference 3 [including a random single failure.] [The failure of a GDCS injection secondary line injection valve results in the greatest reduction in the GDCS reflood rate.]

The LCO requirement for [three] GDCS equalizing trains satisfies the assumptions in Reference 3 for a LOCA initiated by a break in one of the GDCS equalizing lines and a single random failure results in the failure of a second GDCS equalizing line. In this scenario, the [1] remaining GDCS equalizing line is sufficient to satisfy accident analysis assumptions in Reference 3.

The LCO requirement for the ADS function of [ten] S/RVs and [eight] DPVs satisfies the assumptions in Reference 3 for the required depressurization following a small break LOCA assuming a single random failure of one DPV valve. Therefore, the ADS and GDCS will satisfy the limits specified in 10 CFR 50.46 for ECCS during an LOCA concurrent with the worst case single failure if LCO requirements are met.

Note that OPERABILITY of the squib-actuated DPV and GDCS valves requires electrical continuity of [both] redundant explosive charge firing circuits to each valve [except that one squib charge may be bypassed intermittently under administrative controls for required testing or maintenance as specified in SR 3.5.1.4].

OPERABILITY of the GDCS requires that water level in each of the GDCS pools is within the limit specified by SR 3.5.1.1. Additionally, all GDCS RPV block valves, GDCS pool block valves, and suppression pool block valves must be locked open.

OPERABILITY of the ADS function of the S/RVs requires ADS S/RV nitrogen receiver pressure is within the limit specified by SR 3.5.1.2. Additionally, the two solenoid-operated pilot valves on each S/RV actuated by the SSLC logic must be OPERABLE [except that one may be bypassed for performance of required testing or maintenance]. [The DPS is not required to satisfy the assumptions in any accident analysis. Therefore, the solenoid-operated pilot valve on each S/RV actuated by the DPS logic is not required for ADS OPERABILITY.]

APPLICABILITY

All ECCS 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. ECCS requirements for MODES 5 and 6 are specified in LCO 3.5.2, “ECCS - Shutdown.”

ACTIONS

A.1

If one secondary line of one GDCS short-term cooling (injection) train is inoperable, the remaining [seven] GDCS injection secondary lines are sufficient to meet the assumptions in the analysis described in Reference 3 including a single failure that disables one of the remaining GDCS injection secondary lines or a LOCA initiated by a break in one of the OPERABLE GDCS injection secondary lines. In this scenario, restoration of the required GDCS injection secondary line must be completed prior to entering MODE 2 or MODE 4 from MODE 5 (typically the next refueling outage). This Completion Time for this Condition is acceptable because the plant still has enough GDCS injection secondary lines to meet the assumptions in the analysis described in Reference 3 including either a single failure that disables one of the remaining GDCS injection secondary lines. A LOCA initiated by a break in one of the OPERABLE GDCS injection secondary lines in conjunction with a single failure in one of the other GDCS injection secondary lines is not addressed because of the low probability for the combination of these events.

Required Action A.1 is modified by a Note that states that the provisions of LCO 3.0.4.c are applicable. This Note will allow a MODE change when in Condition A, except entering MODE 2 or MODE 4 from MODE 5 is permitted. This is acceptable because the plant still has enough GDCS injection secondary lines to meet the assumptions in the analysis described in Reference 3 when in Condition A.

B.1

If one required GDCS long-term cooling (equalizing) train is inoperable, the remaining [two] GDCS equalizing trains are sufficient to meet the assumptions in the analysis described in Reference 3 including either a single failure that disables one of the remaining GDCS equalizing trains or a LOCA initiated by a break in one of the OPERABLE GDCS equalizing trains. In this scenario, restoration of the required inoperable GDCS equalizer line must be completed prior to entering MODE 2 or MODE 4 from MODE 5 (typically the next refueling outage). This Completion Time for this Condition is acceptable because the plant still has enough GDCS equalizing trains to meet the assumptions in the analysis described in Reference 3 for a LOCA initiated by a break in one of the OPERABLE GDCS equalizing trains or a single failure that disables one of the remaining GDCS equalizing trains during a LOCA. A LOCA initiated by a break in one of the OPERABLE GDCS equalizing lines in conjunction with a single failure in one of the other GDCS equalizing lines is not addressed because of the low probability for the combination of these events.

Required Action B.1 is modified by a Note that states that the provisions of LCO 3.0.4.c are applicable. This Note will allow a MODE change when in Condition A, except entering MODE 2 or MODE 4 from MODE 5 is permitted. This is acceptable because the plant still has enough GDCS injection secondary lines to meet the assumptions in the analysis described in Reference 3 when in Condition B.

C.1

If one short-term cooling (injection) train of GDCS (i.e., two GDCS injection secondary lines) is inoperable, the plant may no longer have the ability to tolerate a single failure in any other GDCS injection secondary lines and remain within the assumptions of the analysis described in Reference 3. If two required GDCS long-term cooling (equalizing) trains are inoperable, the plant may no longer have the ability to tolerate a single failure in any other GDCS equalizing line and remain within the assumptions of the analysis described in Reference 3. In either case, the inoperable required GDCS subsystems must be restored to OPERABILITY within 14 days. This is acceptable because remaining GDCS subsystems are highly reliable and the likelihood of an additional failure during a LOCA is small. Additionally, the likelihood of a LOCA during the 14 day Completion Time that would require the GDCS capacity assumed in the analysis is very small.

D.1

If two or more short-term cooling (injection) trains of GDCS are inoperable or three required GDCS long-term cooling (equalizing) trains are inoperable, the plant may not have the minimum GDCS capacity assumed in Reference 3 for a LOCA. Alternately, if the Required Actions and Completion Time of Condition C are not met, the plant has exceeded the time limit determined to be acceptable for operation without the ability to tolerate a single failure of an additional GDCS injection secondary line or GDCS equalizing line during a LOCA. In either case, the plant must be placed in a MODE in which overall plant risk is minimized. This is accomplished by placing the plant in MODE 3 within 12 hours or remaining in MODE 4. 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.

Remaining in the Applicability of the LCO is acceptable because the plant risk in MODE 3 and MODE 4 is similar to or lower than the risk in MODE 5 (Ref. 7) and because the time spent in MODE 3 to perform the necessary repairs to restore the system to OPERABLE status will be short. Going to cold shutdown results in challenges to the shutdown heat removal systems and requires restarting the plant. However, voluntary entry into MODE 5 may be made, as it is also an acceptable low-risk state.

E.1

If one required ADS valve is inoperable, the plant may no longer have the ability to tolerate a single failure in an ADS valve during a [small break] LOCA. Therefore, the inoperable required ADS valve must be restored to OPERABILITY within 14 days. This Completion Time is acceptable because remaining ADS S/RVs and DPVs are highly reliable and the likelihood of an additional failure during a [small break] LOCA is small. Additionally, the likelihood of a limiting [small break] LOCA that would require the depressurization capacity of all of the ADS valves assumed in the analysis is very small during the 14 day Completion Time.

F.1

If [two] or more required ADS valves are inoperable, the plant may not have sufficient capacity to depressurize the RPV within the time assumed in the analysis for a [small break] LOCA. Alternately, if the Required Actions and Completion Time of Condition E not met, the plant has exceeded the time limit determined to be acceptable for operation without the ability to tolerate a single failure of an additional ADS valve during the [small break] LOCA. In either case, the plant must be placed in a MODE in which overall plant risk is minimized. This is accomplished by placing the plant in MODE 3 within 12 hours or remaining in MODE 4. 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.

Remaining in the Applicability of the LCO is acceptable because the plant risk in MODE 3 and MODE 4 is similar to or lower than the risk in MODE 5 (Ref. 7) and because the time spent in MODE 3 to perform the necessary repairs to restore the system to OPERABLE status will be short. Going to cold shutdown results in the loss of steam-driven systems, challenges the shutdown heat removal systems, and requires restarting the plant. However, voluntary entry into MODE 5 may be made, as it is also an acceptable low-risk state.

SURVEILLANCE REQUIREMENTS

SR 3.5.1.1

This SR requires periodic verification that the water level in each of the GDCS pools is greater than or equal to the specified limit. [The minimum specified level ensures sufficient driving head is available to establish required flow for core cooling following a LOCA. The minimum specified level also 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 highly reliable GDCS pool low level alarms will provide prompt notification of an abnormal level in any of the GDCS pools.

SR 3.5.1.2

This SR requires periodic verification that the supply pressure to ADS S/RVs (i.e., High Pressure Nitrogen Supply System (HPNSS)) is greater than or equal to the specified limit. An accumulator on each ADS S/RV provides pneumatic pressure for ADS valve actuation. The specified HPNSS supply pressure will maintain each ADS S/RV accumulator at a pressure such that, following a failure of HPNSS, each ADS S/RV accumulator contains sufficient energy for at least one valve actuation with the drywell at design pressure or five valve actuations with the drywell at atmospheric pressure. The ECCS safety analysis assumes only one actuation to achieve the depressurization required for operation of the GDCS following a small break LOCA.

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 3.5.1.3

This SR requires periodic verification that each ECCS 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 ADS or GDCS. This SR does not apply to valves that are locked, sealed, or otherwise secured in position because these were verified to be in the correct position when locked, sealed, or secured. A sealed valve utilizes a device that provides evidence of unauthorized manipulation (e.g., cable secured by means of a lead seal).

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. Because of the simplicity of the ADS and GDCS designs and the requirement that block valves for the RPV, GDCS pool, and suppression pool must be locked open, this SR will require periodic verification of very few valves. This SR does not apply to squib-actuated valves.

The 31 day Frequency is acceptable based on engineering judgment and was chosen to provide added assurance that ECCS valves are correctly positioned.

SR 3.5.1.4

This SR requires a periodic verification of the continuity of each of the redundant circuits that initiate the explosive charge for squib-actuated valves in the ADS and GDCS. This periodic verification works in conjunction with the Inservice Test Program. The combination of SR 3.5.1.4 and the Inservice Test Program provides a very high degree of assurance that the explosive charges will function and squib-actuated valves will open when actuated.

The 31 day Frequency is based on operating experience that has demonstrated the reliability of the explosive charge.

The applicable ASME OM-10 Code requirements for squib valves are specified in paragraph 4.6, Inservice Tests for Category D Explosively Actuated Valves (Ref. 6).

SR 3.5.1.5

This SR requires periodic verification that the ADS function of each S/RV actuates on an actual or simulated automatic initiation signal. The ADS function of each S/RV is required to actuate automatically to perform its design function. This test overlaps Surveillance Testing required in the instrumentation section of the Technical Specifications and is intended to provide complete testing of the assumed safety function.

This SR is modified by a Note that excludes ADS S/RV valve actuation as a requirement for this SR to be met. This is acceptable because the valve actuation is verified by SR 3.5.1.7.

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 3.5.1.6

This SR requires periodic verification that that each GDCS valve and the ADS function of each DPV actuates on an actual or simulated automatic initiation signal. The GDCS and ADS functions of each DPV are required to actuate automatically to perform their design functions. This test overlaps Surveillance Testing required in the instrumentation section of the Technical Specifications and is intended 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 3.5.1.4 and the Inservice Test Program for squib-actuated valves.

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. From past operating experience it is believed that these components will pass the SR when performed once per the 24 month refueling interval.

SR 3.5.1.7

This SR requires periodic verification that each ADS S/RV opens when actuated using a manually initiated signal. The ADS S/RV actuation is performed to verify that the valve and solenoids are functioning properly and that no blockage exists in the S/RV discharge lines. S/RV actuation is demonstrated by actual valve stem movement (as indicated by position sensor) or by any other method suitable to verify steam flow.

The S/RV manufacturer recommends that S/RVs not be actuated unless steam pressure is ≥ [6.2] MPa gauge ([900] psig). Meeting this recommendation requires that the reactor be placed in a MODE where the SR is applicable before the conditions for performing the SR are established. Therefore, this SR is modified by a Note stating that the SR is required to be performed within 12 hours after reactor dome pressure is ≥ [6.2] MPa gauge ([900] psig). This Note allows entry into MODES where the SR is applicable without the SR being completed; however, the SR must be completed for each S/RV within 12 hours after the minimum conditions for performing the SR are achieved. Operation in the applicable MODES for a short period of time without this SR completed is acceptable because of the following: there is a low likelihood of a LOCA requiring ADS actuation during this period; the ADS S/RVs are highly reliable and typically pass the SR when it is performed; the redundancy and diversity provided by [10] ADS S/RVs and [8] DPVs minimizes the consequences of an individual ADS S/RV failure; and, the decay heat load is significantly reduced following shutdown where ADS S/RV testing is required. Additionally, S/RV OPERABILITY and the setpoints for overpressure protection are verified prior to valve installation.

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.

This SR verifies S/RV actuation that can be initiated by any of three solenoid-operated pilot valves. Two of the solenoids are actuated by the SSLC logic and the third is actuated by the DPS logic. Therefore, the SR Frequency requires that the SR be performed 24 months on a STAGGERED TEST BASIS for each valve solenoid to ensure that each of the three solenoids are used to initiate valve actuation every third cycle. This is acceptable because OPERABILITY of the solenoid-operated pilot valves is verified as part of SR 3.5.1.5 and is not included in this SR, which verifies OPERABILITY of the valve only.

REFERENCES

1. Chapter 6.
2. Chapter 4.
3. Chapters 6 and 15.
4. 10 CFR 50, Appendix K.
5. 10 CFR 50.46.
6. ASME/ANSI, Operations and Maintenance Standards, Part 10 (OM-10), “Inservice Testing of Valves in Light-Water Reactor Power Plants,” 1988 Adenda.
7. [Topical Report with Technical Justification to Support Risk-Informed End States for ESBWR Plants is under development.]

B 3.5 EMERGENCY CORE COOLING SYSTEMS (ECCS)

B 3.5.2 ECCS - Shutdown

BASES

BACKGROUND	A description of the Gravity-Driven Cooling System (GDCS) is provided in the Bases for LCO 3.5.1, "ECCS - Operating." In MODES 1, 2, 3 or 4, long-term core cooling is provided by the suppression pool via the equalizer lines. Cooling water from the suppression pool is replenished by various means such as GDCS pool dump, ADS valve actuation, Passive Containment Cooling System (PCCS), and the Isolation Condenser System (ICS). If a LOCA or an inadvertent draindown occurs while in MODES 5 or 6, the normal suppression pool level may not be adequate for long-term core cooling and must be replenished by other sources. Due to the reactor pressure and temperature conditions in MODES 5 or 6, the suppression pool will not be replenished by PCCS, ICS, or ADS valve actuation. Therefore, suppression pool cooling water must be replenished by water from the GDCS pools. Two GDCS pools will provide enough water to fulfill the long-term core cooling function for the worst case shutdown LOCA (i.e., [an RWCU drain line break]). Two GDCS pools with a minimum combined volume of [m^3 ( ) ft^3)] provide [sufficient water to flood the lower drywell to a level above the core].
APPLICABLE SAFETY ANALYSES	The ECCS performance is evaluated for the entire spectrum of break sizes for a postulated LOCA. The long-term cooling analysis following a design basis LOCA demonstrates that [one open secondary line from each of two GDCS pools and one open equalizer line from the suppression pool], are required, post-LOCA, to maintain the peak cladding temperature below the allowable limit. To provide redundancy, two GDCS trains are required to be OPERABLE in MODES 5 and 6. These OPERABILITY requirements ensure adequate inventory makeup to the reactor pressure vessel (RPV) in the event of an inadvertent vessel draindown. The ECCS satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).
LCO	In MODES 5 and 6, [two] trains of the ECCS Gravity-Driven Cooling System (GDCS) short-term cooling (injection) subsystem capable of injecting a combined volume of ≥ [m^3 ( ) ft^3)] from associated GDCS pools are required to be OPERABLE.

BASES

Although two GDCS pools are required to provide long-term cooling water during a LOCA, only one of the two secondary lines per pool [and only one of the two equalizer lines] are needed to supply the water to the vessel. This ensures that a single failure of a secondary line [or an equalizer line] will not prevent automatic initiation and successful operation of the minimum required ECCS cooling flow paths.

APPLICABILITY

Two GDCS divisions 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 case of a LOCA or an inadvertent draindown of the vessel. These requirements are not applicable when the new fuel pool gate is removed and water level is ≥ [7.01] meters ([23] feet) over the top of the reactor pressure vessel flange.

Requirements for OPERABILITY of the GDCS and ADS during MODES 1, 2, 3 and 4 are discussed in the Applicability section of the Bases for LCO 3.5.1. The ADS is not required to be OPERABLE in MODES 5 and 6 because the reactor vessel is already depressurized.

ACTIONS

A.1

If one secondary line of one required GDCS short-term cooling (injection) train is inoperable, the inoperable secondary line must be restored to OPERABLE status within 14 days. In this Condition, the remaining OPERABLE secondary line(s) in each of the required GDCS divisions will provide sufficient RPV flooding capability to recover from a LOCA or inadvertent vessel draindown. However, overall ECCS reliability is reduced because a single failure in the remaining OPERABLE secondary line, concurrent with a LOCA or a vessel draindown, could result in the ECCS not being able to perform its intended safety function. The 14 day Completion Time for restoring the required secondary line to OPERABLE status is based on engineering judgment that considered the availability of the remaining OPERABLE secondary line and the low probability of a concurrent LOCA or vessel draindown event.

B.1 and B.2

If the LCO is not met for reasons other than Condition A, action must be initiated to provide within 4 hours at least two method of injecting into the RPV a minimum volume of [m^3 ( ) ft^3)]. In addition, compliance with the LCO must be restored within 72 hours. The Completion Times are considered reasonable based on the probability of a LOCA or vessel draindown event.

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 should be the most prudent and the safest choice, based upon plant conditions.

C.1 and C.2

If Required Actions and associated Completion Times for Conditions A or B are not met, the water inventory available for injection may not be sufficient for a LOCA or draindown event. Therefore, actions must to suspend operations with a potential for draining the reactor vessel (OPDRVs) must be initiated immediately to minimize the probability of a vessel draindown and the potential for subsequent fission product release. Actions must continue until OPDRVs are suspended. In addition, action must be initiated immediately to restore Reactor Building to OPERABLE status as described in the Bases for LCO 3.6.3.1, "Reactor Building." 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 considered reasonable based on the probability of a LOCA or vessel draindown event.

SURVEILLANCE REQUIREMENTS

SR 3.5.2.1

This SR requires periodic verification that the water level in each of the GDCS pools is greater than or equal to the specified limit. [The minimum specified level ensures sufficient driving head is available to establish required flow for core cooling following a LOCA. The minimum specified level also 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 for a minimum of 72 hours without operator intervention.]

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.

BASES

SR 3.5.2.2

This SR requires periodic verification that each ECCS 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 GDCS. This SR does not apply to valves that are locked, sealed, or otherwise secured in position because these were verified to be in the correct position when locked, sealed, or secured. A sealed valve utilizes a device that provides evidence of unauthorized manipulation (e.g., cable secured by means of a lead seal). This SR does not apply to squib-actuated valves.

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. Because of the simplicity of the GDCS design and the requirement that block valves for the RPV, GDCS pool, and suppression pool must be locked open, this SR will require periodic verification of very few valves.

The 31 day Frequency is acceptable based on engineering judgment and was chosen to provide added assurance that ECCS valves are correctly positioned.

SR 3.5.2.3

This SR requires a periodic verification of the continuity of each of the redundant circuits that initiate the explosive charge for squib-actuated valves in the ADS and GDCS. This periodic verification works in conjunction with the Inservice Test Program. The combination of SR 3.5.1.4 and the Inservice Test Program provides a very high degree of assurance that the explosive charges will function and squib-actuated valves will open when actuated.

The 31 day Frequency is based on operating experience that has demonstrated the reliability of the explosive charge.

The applicable ASME OM-10 Code requirements for squib valves are specified in paragraph 4.6, Inservice Tests for Category D Explosively Actuated Valves (Ref. 2).

BASES

REFERENCES

1. Chapter 6.

2. ASME/ANSI, *Operations and Maintenance Standards*, Part 10 (OM-10), "Inservice Testing of Valves in Light-Water Reactor Power Plants," 1988 Adenda.

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 Accident (DBA) and to limit the release of radioactive material to within the requirements of [10 CFR 50.67 (Ref. 1) or the NRC Staff-approved licensing basis]. The containment consists of a steel-lined, reinforced concrete vessel, which surrounds the reactor coolant system and provides an essentially leak-tight barrier against an uncontrolled release of radioactivity to the environment. To ensure the containment is OPERABLE, leakage test requirements have been established by Reference 2, which requires periodic verification of the leak-tight integrity of the containment and of the systems and components that penetrate the containment. The leakage tests ensure that leakage through the containment and through systems and components penetrating the containment do not exceed the allowable leakage rates specified in the Containment Leakage Rate Testing Program and used in the safety analyses. Additionally, the periodic tests ensure that proper maintenance and repairs are made during the service life of the plant. This specification ensures that the performance of the containment meets the assumptions used in the safety analyses of References 3 and 4 during a DBA. All leakage rate surveillance requirements are in conformance with 10 CFR 50, Appendix J (Ref. 2), as modified by approved exemptions described in the Containment Leakage Rate Testing Program.
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 release of fission-product radioactivity subsequent to a DBA will not result in doses in excess of the values given in the licensing basis assuming the availability of the engineered safety feature (ESF) systems. 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

BASES

fission products to the environment is controlled by the rate of containment leakage.

Analytical methods and assumptions involving the containment are presented in References 3 and 4. The safety analyses assume a non-mechanistic fission-product release following a DBA that forms the basis for determination of off-site 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 50.67] (Ref. 1) even if the non-mechanistic release were to occur.

The maximum allowable leakage rate for the containment is 0.5% by weight of the containment air per 24 hours at the maximum calculated containment pressure (Ref. 3), excluding MSIV leakage. The maximum allowable leakage rate is based on what is acceptable for nuclear safety considerations per [10 CFR 50.67] (Ref. 1). Reactor size, site location, and meteorology, as well as the possible mechanisms for radioactivity generation and transport, are all considered in specifying the allowable leakage rate for a given containment system.

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

LCO

This LCO requires that the containment is OPERABLE. Containment OPERABILITY is maintained by limiting leakage to within the acceptance criteria of 10 CFR 50, Appendix J (Ref. 2). The containment design leakage rate is an assumed initial condition. The requirements stated with this LCO define the performance of the containment fission-product barrier.

The containment LCO requires that containment OPERABILITY be maintained. Other containment LCOs support this LCO by ensuring that:

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 deactivated automatic valves secured in their closed positions, except as provided in LCO 3.6.1.3.

BASES

b. The containment air lock is OPERABLE except as provided in LCO 3.6.1.2.

c. The sealing mechanism associated with each penetration (e.g., welds, bellows, or O-rings) is OPERABLE.

The Required Actions when other containment LCOs are not met have been specified in those LCOs and not in LCO 3.6.1.1.

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.

B.1

If containment cannot be restored to OPERABLE status in the required Completion Time, the plant must be placed in a MODE in which overall plant risk is minimized. This is accomplished by placing the plant in MODE 3 within 12 hours or remaining in MODE 4. 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

Remaining in the Applicability of the LCO is acceptable because the plant risk in MODE 3 and MODE 4 is similar to or lower than the risk in MODE 5 (Ref. 5) and because the time spent in MODE 3 to restore drywell pressure to within the specified limit will be short. Going to cold shutdown results in challenges to the shutdown heat removal systems and requires restarting the plant. However, voluntary entry into MODE 5 may be made, as it is also an acceptable low-risk state.

SURVEILLANCE REQUIREMENTS

SR 3.6.1.1.1

This SR requires performing visual examinations and leakage rate testing, except for containment air lock testing, 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 containment OPERABLE requires compliance with requirements of 10 CFR 50, Appendix J (Ref. 2), as modified by approved exemptions, which are identified in the Containment Leakage Rate Testing Program.

This SR includes the leakage rate for the overall containment (Type A leakage tests) including leakage from equipment hatches, electrical penetrations with resilient seals, and other penetrations. Air lock door seal leakage testing (Type B leakage tests) is addressed in LCO 3.6.1.2. Leakage from CIVs (Type C leakage tests) is addressed in LCO 3.6.1.3.

The Frequency is specified in the Containment Leakage Rate Testing Program.

SR 3.6.1.1.2

This SR measures drywell-to-suppression wetwell differential pressure during a [10] minute period to ensure that the leakage paths that would bypass the suppression pool are within allowable limits. Limiting the leakage from the drywell to the suppression wetwell is necessary for the functioning of the pressure suppression function of the containment. This ensures that the steam produced by an event that pressurized the drywell will be directed through the pressure suppression vent system into the suppression pool.

This SR is performed by establishing a known differential pressure between the drywell and the suppression wetwell and verifying that the pressure in either the suppression wetwell or the drywell does not change

BASES

by more than 6 mm water (0.25 inches water) per minute over a 10 minute period at an initial differential pressure of 6.9 kPa (1 psi).

The 24 month Frequency is acceptable because [SR 3.6.1.6.1] requires verification every 14 days that each suppression wetwell to drywell vacuum breaker is closed, 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.]

Two consecutive failures of this SR are an indication of unexpected containment degradation. In this event, test Frequency must be increased to once every 12 months until the situation is remedied as evidenced by passing two consecutive tests.

REFERENCES

1. [10 CFR 50.67]
2. 10 CFR 50, Appendix J, “Primary Reactor Containment Leakage Testing for Water Cooled Power Reactors.”
3. [Section 6.2].
4. [Section 15.1].
5. [Topical Report with Technical Justification to Support Risk-Informed End States for ESBWR Plants is under development.]

B 3.6 CONTAINMENT SYSTEMS

B 3.6.1.2 Containment Air Lock

BASES

BACKGROUND

[Two] double-door containment air locks 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 in order to maintain containment integrity (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-gasketed 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. Additionally, control room indication is provided to alert the operator whenever an air lock door interlock mechanism is defeated. 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 off-site doses from a DBA. Not maintaining air lock integrity or air tightness may result in off-site doses in excess of those described in the plant safety analyses. All leakage rate surveillance requirements conform to 10 CFR 50, Appendix J (Ref. 2), as modified by approved exemptions,

BASES

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 [0.5%] by weight of the containment per 24 hours at the calculated maximum containment pressure (Ref. 1), excluding MSIV leakage. This allowable leakage rate forms the basis for the acceptance criteria imposed on the SRs associated with the air lock. Containment air lock OPERABILITY is also required to minimize the amount of fission-product gases that may bypass containment to contaminate and pressurize the [safety envelope].

The containment air lock satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

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 10 CFR 50, Appendix J, 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 will support containment integrity because each door is designed to withstand the peak containment pressure calculated to occur following a DBA. However, both doors are kept closed when the air lock is not being used to enter or exit the containment.

The air lock interlock mechanism allows only one air lock door to be opened at one time. Thus, the door interlock feature supports containment integrity while the air lock is being used for personnel transit in and out of the containment.

This LCO provides assurance that the containment air lock will perform its designed safety function to mitigate the consequences of accidents that could result in off-site exposures comparable to [10 CFR 50.67 limits or some fraction as established in an NRC staff-approved licensing basis].

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 airlocks 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 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.

Required Action A.2 specifies the air lock must be isolated by locking closed the OPERABLE air lock door within the 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.

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 airlock 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 airlock 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.

Note 2 provides an allowance that entry and exit using an inoperable airlock 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>C.1, C.2, and C.3</u>

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.

D.1

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 overall plant risk is minimized. This is accomplished by placing the plant in MODE 3 within 12 hours or remaining in MODE 4. 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.

Remaining in the Applicability of the LCO is acceptable because the plant risk in MODE 3 and MODE 4 is similar to or lower than the risk in MODE 5 (Ref. 4) and because the time spent in MODE 3 to restore drywell pressure to within the specified limit will be short. Going to cold shutdown results in challenges to the shutdown heat removal systems and requires restarting the plant. However, voluntary entry into MODE 5 may be made, as it is also an acceptable low-risk state.

SURVEILLANCE REQUIREMENTS

SR 3.6.1.2.1

This SR requires periodic verification that the airlocks are in compliance with the leakage rate test requirements of 10 CFR 50, Appendix J, as modified by approved exemptions described in the 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

BASES

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 airlock leakage rate testing be evaluated as part of the acceptance criteria applicable to SR 3.6.1.1.1.

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 Frequency is based on engineering judgment and is acceptable because the interlock mechanism is typically not challenged when containment is entered because of training and administrative controls. Additionally, indications of airlock door and interlock mechanism status would alert operators promptly of a failure of an interlock.

REFERENCES

1. Section 6.2.

2. 10 CFR 50, Appendix J, “Primary Reactor Containment Leakage Testing for Water-Cooled Power Reactors.”

3. [10 CFR 50.67]

4. [Topical Report with Technical Justification to Support Risk-Informed End States for ESBWR Plants is under development.]

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 50.67 (Ref. 1) off-site dose limits that are part of the NRC staff-approved licensing basis]. The OPERABILITY requirements for CIVs help ensure that adequate containment leaktightness 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. 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. One of these barriers may be a closed system inside containment.

The CIVs are required by General Design Criteria (GDC) 54, 55, 56, and 57 (Ref. 2). These GDCs set guidelines for the isolation capability of lines that penetrate containment. The requirements differentiate between lines that connect to the containment air space, lines that connect to the reactor coolant pressure boundary, and lines that connect to some other component inside containment. The GDC include requirements for design and leakage.

This LCO is intended to ensure that the GDC requirements are satisfied during plant operation.

BASES

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 50.67 (Ref. 1), a proposed site must consider a fission-product release from the core, with off-site release based on the expected demonstrable leakage rate from the containment. This LCO is intended to ensure that off-site dose limits are not exceeded (i.e., the actual containment leakage rate does not exceed the value assumed in the safety analyses). As part of the containment boundary, CIV and containment purge isolation valve OPERABILITY are 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, a main feedwater line break (MFLB), 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. Of the events analyzed in Reference 3, [the MSLB is the most limiting event] based on the radiological consequences. The [closure time of the main steam isolation valves (MSIVs)] is the most significant variable from a radiological standpoint. The MSIVs are required to close in [> 3 but < 4.5 seconds]; therefore, the [4.5-second] closure time is assumed in the analysis. The off-site dose calculations assume that the purge valves were closed at event initiation. 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 that within [30] seconds of the accident, isolation of the containment is complete and leakage is terminated, except for the design leakage rate. The containment isolation total response time of 30 seconds 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.

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 off-site radiation exposures resulting from a DBA. This LCO provides assurance that the CIVs will perform their designed safety functions to

BASES

mitigate the consequences of accidents that could result in off-site exposure.

This LCO addresses CIV OPERABILITY including stroke time and leakage. LCO 3.6.1.1, “Containment,” address other CIV leakage rates under Type C testing.

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 actuate within the required differential pressure range. The valves covered by this LCO are listed with their associated stroke times in Reference 5.

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 and closed systems are in place. The passive isolation valves/devices are those listed in Reference 5.

APPLICABILITY

CIVs must be OPERABLE in MODES 1, 2, 3, and 4 when a DBA could cause a 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 most CIVs is not required to ensure containment integrity when in MODE 5 or 6. Certain valves, however, are required to be OPERABLE in MODES 5 and 6 to prevent inadvertent reactor vessel draindown. These valves are those associated with instrumentation required to be OPERABLE per LCO 3.3.6.1 and 3.3.6.2 to isolate the Reactor Water Cleanup/Shutdown Cooling Lines on [Reactor Vessel Water Level [and] Level 2 Reactor Vessel Water Level , Level 2].

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.

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.

A.1 and A.2

Condition A is applicable only to those penetration flow paths with two CIVs. For penetration flow paths with one CIV, Condition C provides the appropriate Required Actions.

If one of the CIVs is inoperable in one or more penetration flow paths is inoperable for reasons other than Condition D, the penetration still has isolation capability but the ability to tolerate a single failure is lost. Therefore, Required Action A.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 A.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 CIV, 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 before the initiating the transient associated with MSL isolation. This is acceptable because the penetration still has isolation capability although the ability to tolerate a single failure is lost.

Required Action A.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, through a system walkdown, 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 of for verification of isolation valves inside containment is that verification must be completed prior to entering MODE 2 or 3 from MODE 4 if containment was de-inerted while in MODE 4 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.

Condition A is not applicable to excess flow check valves (EFCVs) that isolate protection system instruments. Condition C provides the appropriate Required Actions for inoperable EFCVs. EFCVs are associated with instruments in systems such as the Reactor Trip System, Emergency Core Cooling System, Containment Isolation System, safety/relief valves, anticipated transient without scram, and feedwater/main turbine trip.

[Periodic verification of valves and blind flanges located in high radiation areas may be verified closed by use of administrative controls. Allowing verification by administrative controls 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.]

B.1

Condition B is applicable only to those penetration flow paths with two CIVs. For penetration flow paths with one CIV, Condition C provides the appropriate Required Actions.

If two CIVs are inoperable in one or more penetration flow paths (for reasons other than Condition D), isolation capability for the penetration is lost. Therefore, at least one of the CIVs in each flow path must be restored to OPERABLE within one hour or Required Action B.1 requires that the penetration be isolated within one hour.

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 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 CIV, a closed manual valve, a check valve with flow through the valve secured, or a blind flange.

The Completion Time of one hour is acceptable because it 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.

[Periodic verification of valves and blind flanges located in high radiation areas may be verified closed by use of administrative controls. Allowing verification by administrative controls 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.]

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

Condition C is applicable only to those penetration flow paths with one CIV. This Condition is written to specifically address those penetrations isolated in accordance with 10 CFR 50, Appendix A, GDC 57 (Ref. 2). GDC 57 allows those lines that penetrate containment but are neither part of the reactor coolant pressure boundary nor connected directly to the containment atmosphere to be isolated by means of one CIV. For penetration flow paths with two CIVs, Conditions A and B provide the appropriate Required Actions.

If the CIV is inoperable in one or more penetration flow paths (for reasons other than Condition D), isolation capability is degraded. Therefore, Required Action C.1 specifies that the affected penetrations must be isolated within 4 hours except for penetrations with EFCVs or penetrations for closed systems. Penetrations with EFCVs and penetrations for closed systems must be isolated within 72 hours.

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 single active failure. Isolation barriers that meet this criterion are a closed and deactivated automatic CIV, a closed manual valve, or a blind flange.

A check valve may not be used to isolate the affected penetration, because GDC 57 (Ref. 2) does not consider the check valve an acceptable automatic isolation valve.

The Completion Time of 72 hours to isolate penetrations with closed systems is acceptable because of the relative reliability of the closed system as a penetration isolation boundary. The Completion Time of 72 hours to isolate penetrations with EFCVs is needed because closure of these valves may result in an unplanned transient

Required Action C.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, through a system walkdown, 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.

<u>D.1</u>

If CIV 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. 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 hydrostatically tested lines [not on a closed system] is 4 hours. The Completion Time for restoration of reactor building bypass leakage is 4 hours. The Completion Time for restoration of Main Steam Isolation Valve leakage is 8 hours. The Completion Time for restoration of hydrostatically tested lines [on a closed system] is 72 hours. Each of these completion times is consistent

BASES

with the Completion Time for isolation of an inoperable valve of the same type.

E.1

If a Required Action and associated Completion Time of Condition A, B, C, or D is not met in MODE 1, 2, 3, or 4, the plant must be placed in a MODE in which overall plant risk is minimized. This is accomplished by placing the plant in MODE 3 within 12 hours or remaining in MODE 4. 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.

Remaining in the Applicability of the LCO is acceptable because the plant risk in MODE 3 and MODE 4 is similar to or lower than the risk in MODE 5 (Ref. 3) and because the time spent in MODE 3 to restore drywell pressure to within the specified limit will be short. Going to cold shutdown results in challenges to the shutdown heat removal systems and requires restarting the plant. However, voluntary entry into MODE 5 may be made, as it is also an acceptable low-risk state.

F.1

If a Required Action and associated Completion Time of Condition A, B, C, or D is not met during MODE 5 or 6, the potential exists for a loss of coolant inventory. Therefore, action must be initiated immediately to OPDRVs and to restore the inoperable valves to OPERABLE status.

SURVEILLANCE REQUIREMENTS

SR 3.6.1.3.1

This SR requires periodic verification that each [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 [500 mm (20 in)] inch 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.

[Alternate SR][This SR requires periodic verification that each [500 mm (20 in)] containment purge valve is closed. This SR is designed to ensure that an inadvertent or spurious opening of a primary containment purge valve does not cause a gross breach of primary containment. Detailed analysis of the purge valves failed to conclusively demonstrate their ability to close during a LOCA in time to limit offsite doses. Primary containment purge valves that are sealed closed must have motive power to the valve operator removed. This can be accomplished by de-energizing the source of electric power or removing the air supply to the valve operator. In this application, the term "sealed" has no connotation of leak tightness. 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 a result of an NRC initiative, Generic Issue B-24 (Ref.[ ]) related to primary containment purge valve use during unit operations.]

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 [and a highly reliable alarm will alert operations personnel of abnormal containment purge valve position or valve alignment.

<u>SR 3.6.1.3.2</u>

This SR requires periodic verification that each containment isolation manual valve 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, through a system walkdown, 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.

SR 3.6.1.3.3

This SR requires periodic verification that each containment isolation manual valve 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 3.6.1.3.4

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 3.6.1.3.5.

The Frequency for this SR is in accordance with the requirements of the Inservice Testing Program of 92 days.

SR 3.6.1.3.5

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. This ensures that the calculated radiological consequences of these events remain within [10 CFR 50.67] limits.

The 24 month Frequency is consistent with the requirements of the Inservice Testing Program.

SR 3.6.1.3.6

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.

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 3.6.1.3.7

This SR requires periodic verification that a representative sample of reactor instrumentation line excess flow check valves (EFCVs) each reduce flow to ≤ [3.79 liters/hour (1 gph)] on a simulated line break. This SR provides assurance that the instrumentation line excess flow check valves will perform so that predicted radiological consequences will not be exceeded during the postulated instrumentation line break event evaluated in Reference 4.

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.

SR 3.6.1.3.8

This SR requires periodic verification that the leakage rate through each MSIV is within the specified limit. The analyses in References 3 and 4 are based on leakage that is less than the specified limit.

The MSIV leakage rate 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 MSIVs OPERABLE requires compliance with requirements of 10 CFR 50, Appendix J (Ref. 2), as modified by approved exemptions, which are identified in the Containment Leakage Rate Testing Program.

BASES

SR 3.6.1.3.9

This SR requires periodic verification that the leakage through each hydrostatically tested line that penetrates the containment does not exceed [0.227 m^3/hour (1 gpm)] when tested at [1.1 times] peak calculated containment pressure. Note that dual function valves must pass all applicable SRs, including the Type C leakage rate test (SR 3.6.1.1.1), if appropriate.

The leakage rate 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 hydrostatically tested lines OPERABLE requires compliance with requirements of 10 CFR 50, Appendix J (Ref. 2), as modified by approved exemptions, which are identified in the Containment Leakage Rate Testing Program.

SR 3.6.1.3.10

This SR requires periodic verification that the leakage rate for all Reactor Building bypass leakage path[s], except MSIVs, is within limits.

The leakage rate 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 hydrostatically tested lines OPERABLE requires compliance with requirements of 10 CFR 50, Appendix J (Ref. 2), as modified by approved exemptions, which are identified in the Containment Leakage Rate Testing Program.

REFERENCES

1. [10 CFR 50.67.]
2. 10 CFR 50, Appendix A, “General Design Criteria for Nuclear Power Plants.”
3. Section 15.6.
4. Section 6.2.
5. Table 6.2.

BASES

6. Generic Issue B-20, “Containment Leakage Due to Seal Deterioration.”

7. [Generic Issue B-24, “Containment Purge Valve Reliability.”]

8. 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. A positive internal pressure also ensures that air does not leak into the containment that is required to remain inerted. The containment is designed to contain radioactive material that may be released from the reactor core following a Design Basis Accident (DBA). The containment is required to ensure that off-site radiation exposures are maintained within the requirements of [10 CFR 50.67 (Ref. 1) or the NRC staff approved licensing basis].
APPLICABLE SAFETY ANALYSES	Containment performance is evaluated for the entire spectrum of break sizes for postulated loss-of-coolant accidents (LOCAs). The upper limit for containment drywell pressure is an initial condition in the analyses (Ref. 2) that ensures that the peak drywell internal pressure will be maintained below the drywell design pressure in the event of a DBA LOCA. Maintaining the containment drywell pressure within the specified limit ensures that the safety analysis remains valid and ensures that the peak LOCA drywell internal pressure does not exceed the design value for containment pressure of 379 kPa gauge (55 psig). The calculated peak drywell pressure for the limiting event is provided in Reference 2. Drywell pressure satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).
LCO	This LCO requires that containment drywell pressure be maintained ≤ 5.17 kPa gauge (0.75 psig) 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 DBA. As a result, containment integrity is ensured.

BASES

APPLICABILITY

Containment drywell pressure must be maintained within the specified limit in MODES 1, 2, 3, and 4 when a DBA 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 to ensure containment integrity when in MODE 5 or 6.

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

If drywell pressure cannot be restored to within limits in the associated Completion Time, the plant must be placed in a MODE in which overall plant risk is minimized. This is accomplished by placing the plant in MODE 3 within 12 hours or remaining in MODE 4. 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.

Remaining in the Applicability of the LCO is acceptable because the plant risk in MODE 3 and MODE 4 is similar to or lower than the risk in MODE 5 (Ref. 3) and because the time spent in MODE 3 to restore drywell pressure to within the specified limit will be short. Going to cold shutdown results in challenges to the shutdown heat removal systems and requires restarting the plant. However, voluntary entry into MODE 5 may be made, as it is also an acceptable low-risk state.

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.

BASES

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 highly reliable drywell pressure alarms will provide prompt notification of abnormal drywell pressure.

REFERENCES

1. [10 CFR 50.67]

2. Chapter 6.2.

3. [Topical Report with Technical Justification to Support Risk-Informed End States for ESBWR Plants is under development.]

B 3.6 CONTAINMENT SYSTEMS

B 3.6.1.5 Drywell Air Temperature

BASES

BACKGROUND

The average drywell airspace temperature is an initial condition for the analyses for containment performance during postulated accidents and transients (Ref.1). Additionally, drywell airspace temperature may affect equipment OPERABILITY and personnel access.

During normal operation, the reactor vessel and piping add heat to the drywell airspace. Drywell coolers remove heat and maintain a suitable environment. The limit on drywell average air temperature was developed as a reasonable upper bound based on the plant design and operating plant experience. This limit on drywell temperature was then used in the Reference 1 safety analyses.

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 57.2°C (135°F). This limitation ensures that the safety analysis remains valid by maintaining the expected initial conditions and ensures that the peak LOCA drywell temperature does not exceed the maximum allowable of 171°C (340°F) (Ref. 2).

[The most severe drywell temperature condition occurs as a result of a Reactor Coolant System rupture above the reactor water level that results in the blowdown of reactor steam to the drywell. The drywell temperature analysis considers main steam line breaks (MSLBs) occurring inside the drywell and having various break areas. The maximum calculated drywell average temperature for the worst case break area is provided in (Ref. 2).]

[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 ≤ [57.2°C (135°F)].

In the event of a DBA, with an initial drywell average temperature less than or equal to the LCO temperature limit, the resultant peak accident temperature is maintained below the containment design temperature. As a result, the ability of containment to perform its design function is ensured.

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, maintaining suppression pool average temperature within limits is not required in MODES 5 or 6 to ensure containment integrity.

ACTIONS

A.1

If drywell average air temperature 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 the [low] sensitivity of the analysis to variations in this parameter.

B.1

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 overall plant risk is minimized. This is accomplished by placing the plant in MODE 3 within 12 hours or remaining in MODE 4. 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

Remaining in the Applicability of the LCO is acceptable because the plant risk in MODE 3 and MODE 4 is similar to or lower than the risk in MODE 5 (Ref. 3) and because the time spent in MODE 3 to restore drywell pressure to within the specified limit will be short. Going to cold shutdown results in challenges to the shutdown heat removal systems and requires restarting the plant. However, voluntary entry into MODE 5 may be made, as it is also an acceptable low-risk state.

SURVEILLANCE REQUIREMENTS

SR 3.6.1.5.1

This SR requires verification that drywell average air temperature in within specified limits every 24 hours. Drywell air temperature is monitored in all quadrants and at various elevations (referenced to mean sea level). Due to the shape of the drywell, a volumetric average is [is determined automatically by instrumentation that] used to determine an accurate representation of the actual average temperature.

The 24 hour Frequency of the SR is acceptable because (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. Section 6.3.
3. [Topical Report with Technical Justification to Support Risk-Informed End States for ESBWR Plants is under development.]

B 3.6 CONTAINMENT SYSTEMS

B 3.6.1.6 Suppression Wetwell-to-Drywell Vacuum Breakers

BASES

BACKGROUND

The function of the suppression wetwell-to-drywell vacuum breakers is to relieve vacuum in the drywell. There are 3 vacuum breakers between the drywell and the suppression wetwell, which allow air and steam flow from the suppression wetwell to the drywell when the drywell is at a negative pressure with respect to the suppression wetwell. Therefore, suppression wetwell-to-drywell vacuum breakers prevent an excessive negative differential pressure across the wetwell-drywell boundary. Each vacuum breaker is a self-actuating 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. Cooling cycles result in minor pressure transients in the drywell that occur slowly and are normally controlled by heating and ventilation equipment. Spray actuation or spill of subcooled water out of a break result in more significant pressure transients and become important in sizing the vacuum breakers.

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, air in the drywell is purged into the suppression wetwell free airspace, leaving the drywell full of steam. Condensation of the steam caused by ECCS causes depressurization of the drywell.

During normal operation, the drywell-to-suppression wetwell differential pressure determines the height of the water leg in the downcomer vertical vents. If the drywell pressure is less than the suppression wetwell pressure, there will be an increase in the vent water leg. This will result in an increase in the water-clearing inertia in the event of a postulated LOCA resulting in an increase in the peak drywell pressure. This in turn will result in an increase in the pool swell dynamic loads. The vacuum breakers limit the height of the water leg in the vent system during normal operation.

On the upstream side of the vacuum breaker, a DC solenoid operated butterfly valve designed to fail-close is provided. During a LOCA, when the vacuum breaker opens to equalize the suppression wetwell-to-drywell

BASES

	pressure and subsequently does not completely close as detected by the proximity sensors, a control signal will close the upstream butterfly valve to prevent extra bypass leakage due to the opening created by the vacuum breaker
APPLICABLE SAFETY ANALYSES	Analytical methods and assumptions involving the suppression wetwell-to-drywell vacuum breakers are presented in Reference 1 as part of the accident response of the containment systems. The vacuum breakers are provided as part of the containment to limit the negative pressure differential across the drywell and suppression wetwell walls that form part of the containment boundary. A DBA 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 that purges the drywell of nitrogen gas and fills the drywell free airspace with steam. 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 fully open at a differential pressure of [3.45 kPa (0.5 psi)]. The analyses also assume that a single failure causes one of the 3 vacuum breakers to fail to open. The analyses show that the drywell-to-suppression wetwell design pressure is not exceeded even under the worst-case accident scenario. The vacuum breaker opening differential pressure and the requirement that all 3 vacuum breakers be operational are a result of the requirement placed on the vacuum breakers to limit the vent system water leg height. The suppression wetwell-to-drywell vacuum breakers satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).
LCO	This LCO requires that all 3 vacuum breakers are closed and OPERABLE for opening. Vacuum breaker OPERABILITY provides assurance that the drywell-to-suppression wetwell negative pressure differential remains below the design value. The requirement that the vacuum breakers be closed ensures that there is no excessive bypass leakage should a LOCA occur.

BASES

APPLICABILITY

Vacuum breaker OPERABILITY must be maintained 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 RPV pressure and temperature are lower. Therefore, maintaining suppression wetwell-to-drywell vacuum breakers OPERABLE is not required in MODE 5 or 6 to ensure containment integrity.

ACTIONS

A.1

If one suppression wetwell-to-drywell vacuum breaker is inoperable because it will not open or the associated block valve in not open, the remaining 2 OPERABLE vacuum breakers are capable of providing the vacuum relief function. However, overall system reliability is reduced because a single failure in one of the remaining vacuum breakers could result in an excessive suppression wetwell-to-drywell differential pressure during a DBA. Therefore, 72 hours is allowed to restore the inoperable vacuum breakers to OPERABLE status (consistent with other containment functions) so that plant conditions are consistent with those assumed for the design basis analysis.

The Completion Time of 72 hours is acceptable because the remaining 2 OPERABLE vacuum breakers are 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.

B.1

If one suppression wetwell-to-drywell vacuum breaker is inoperable because it will not close, there is the potential for suppression wetwell overpressurization due to this bypass leakage if a LOCA were to occur. An open vacuum breaker allows communication between the drywell and suppression wetwell airspace. Therefore, the open vacuum breaker must be closed or isolated within 4 hours.

The Completion Time of 72 hours is acceptable because it allows a short time to test the vacuum breaker position and probability of a LOCA occurring during the short time of the test is low.

Alternate methods for verifying vacuum breaker position may be used if vacuum breaker position indication is inoperable, shows an open vacuum breaker, or is not reliable. The ability to maintain a differential pressure of

BASES

3.45 kPa (0.5 psi) between the suppression wetwell and drywell for one hour without makeup is an adequate demonstration that all vacuum breakers are closed.

C.1

If two suppression wetwell-to-drywell vacuum breakers are inoperable in accordance with either Condition A, Condition B or both, then the remaining OPERABLE vacuum breaker is not capable of providing the required vacuum relief function.

If the Required Action and associated Completion Time of Condition A or B are not met, the plant has exceeded the permitted to attempt restoration of an inoperable vacuum breaker.

In either case, the plant must be placed in a MODE in which overall plant risk is minimized. This is accomplished by placing the plant in MODE 3 within 12 hours or remaining in MODE 4. 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.

Remaining in the Applicability of the LCO is acceptable because the plant risk in MODE 3 and MODE 4 is similar to or lower than the risk in MODE 5 (Ref. 3) and because the time spent in MODE 3 to restore drywell pressure to within the specified limit will be short. Going to cold shutdown results in challenges to the shutdown heat removal systems and requires restarting the plant. However, voluntary entry into MODE 5 may be made, as it is also an acceptable low-risk state

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, or by performing [SR 3.6.1.1.2].

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.

BASES

SR 3.6.1.6.2

This SR requires periodic verification that the isolation valve associated with each vacuum breaker is 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 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 3.6.1.6.3

This SR requires periodic verification of the free movement of each vacuum breaker to ensure they are capable of performing their intended function.

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 breakers 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.

REFERENCES

1. Section 6.2.
2. [10 CFR 50.67.]
3. [Topical Report with Technical Justification to Support Risk-Informed End States for ESBWR Plants is under development.]

B 3.6 CONTAINMENT SYSTEMS

B 3.6.1.7 Passive Containment Cooling System (PCCS)

BASES

BACKGROUND

The Passive Containment Cooling System (PCCS) removes heat from the containment drywell to maintain the pressure and temperature inside the containment within design limits following a Design Basis Accident (DBA). The Passive Containment Cooling System (PCCS) condensers absorb heat from the primary containment following a LOCA [or transient that releases heat to the containment]. The Isolation Condensers (IC) absorb heat from the RCS following a reactor isolation incident [or LOCA]. The ICS/PCCS pool provides a heat sink for both the ICS and PCCS condensers.

The PCCS absorbs some of the sudden input of heat energy from the LOCA steam blowdown into the drywell and then absorbs heat energy from steam generated by fuel decay heat released to the containment. The PCCS is a passive system with no components that must actively function and uses natural circulation to maintain the Containment within its limits for design basis accidents. The determining maximum allowable steam bypass leakage area for ESBWR design, analyses take credit for PCCS operation immediately following LOCA initiation.

The PCCS consists of six elevated heat exchangers (condensers) located outside the containment. The condensers are submerged in a large pool of water (ICS/PCCS pool), which is at atmospheric pressure. Steam produced in ICS/PCCS pool by boiling around the PCCS condensers is vented to the atmosphere. No forced circulation equipment is required for operation of the PCCS. The PCCS is capable of 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.

Each of the 6 PCCS condensers is made of two identical modules. Each PCCS condenser two-module assembly is designed to remove a nominal 11 MWt of decay heat assuming the following: the containment side of the condenser contains pure, saturated steam at 308 kPa absolute (45 psia) and 134°C; and, the ICS/PCCS pool is at atmospheric pressure with a water temperature of 101°C.

The PCCS condensers are an extension of the containment boundary, do not have isolation valves, and start operating immediately following a LOCA. Each PCCS condenser contains a central steam supply pipe that

BASES

is open to the containment drywell at its lower end, and at its upper end feeds two horizontal headers through two branch pipes. Steam is condensed inside vertical tubes and the condensate is collected in two lower headers. The condensate returns by gravity flow to the GDCS pools where it is returned to the RPV via the GDCS injection lines. Noncondensable gases are purged to the suppression pool via vent lines.

The PCCS condenser vent and the drain lines from each lower header are routed to the drywell through a single containment penetration. Spectacle flanges are included in the drain line and in the vent line to conduct post maintenance leakage tests separately from Type A containment leakage tests.

The ICS/PCCS pool, located above, and outside, the containment boundary, provides the heat sink for all 6 PCCS condensers. When maintained at specified levels, the ICS/PCCS pool PCCS is capable of removing sufficient post-LOCA decay heat from the containment to maintain containment pressure and temperature within design limits for a minimum of 72 hours.

Each PCCS condenser is located in a sub-compartment of the ICS/PCCS pool. During a LOCA, pool water temperature could rise to about 101°C (214°F). The steam formed will be non-radioactive and have a slight positive pressure relative to station ambient. The steam generated in the ICS/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 ICS/PCCS pool water.

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 that the PCCS and the ICS/PCCS pool are OPERABLE when required. Each PCCS condenser loops must satisfy all the performance and physical arrangement SRs, including ICS/PCCS pool level, in order to be OPERABLE.

The PCCS capacity needed to maintain containment peak pressure and temperature below design limits (Ref. 1) for at least 72 hours after a LOCA depends on THERMAL POWER prior to the event. Reference 1 indicates that adequate PCCS capacity is maintained with the following restrictions on THERMAL POWER:

- Six (6) PCCS condenser loops must be OPERABLE when the reactor is operating with THERMAL POWER [> 80% RTP];
- Five (5) PCCS condenser loops must be OPERABLE with THERMAL POWER [≤ 80% RTP];
- Four (4) PCCS condenser loops must be OPERABLE with THERMAL POWER [≤ 60% RTP]; and,
- Three (3) PCCS condenser loops must be OPERABLE with THERMAL POWER [≤ 40% RTP];

[Reference 1 does not make any allowance for single failure because the design of the passive PCCS results in no credible failure that will prevent operation of a PCCS condenser loop when required.]

APPLICABILITY

The PCCS and the ICS/PCCS pool are required to be OPERABLE in MODES 1, 2, 3, and 4 because a DBA could cause a pressurization and heat up of 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, passive containment cooling is not required to be OPERABLE in MODES 5 and 6 to prevent leakage of radioactive material from containment.

ACTIONS

A.1

If one PCCS condenser loop is inoperable, passive containment cooling capacity may not be sufficient to meet the containment design requirements unless THERMAL POWER is ≤ 80% RTP. Therefore, at least one inoperable train must be restored to OPERABLE status or THERMAL POWER must be reduced to ≤ 80% RTP within 8 hours. The

Completion Time of 8 hours is acceptable because of the low probability of a DBA occurring during this period.

B.1

If two PCCS condenser loops are inoperable, passive containment cooling capacity may not be sufficient to meet the containment design requirements unless THERMAL POWER is ≤ 60% RTP. Therefore, at least one inoperable train must be restored to OPERABLE status or THERMAL POWER must be reduced to ≤ 60% RTP within 8 hours. The Completion Time of 8 hours is acceptable because of the low probability of a DBA occurring during this period.

C.1

If three PCCS condenser loops are inoperable, passive containment cooling capacity may not be sufficient to meet the containment design requirements unless THERMAL POWER is ≤ 40% RTP. Therefore, at least one inoperable train must be restored to OPERABLE status or THERMAL POWER must be reduced to ≤ 40% RTP within 8 hours. The Completion Time of 8 hours is acceptable because of the low probability of a DBA occurring during this period.

D.1

If four or more PCCS condenser loops are inoperable, the functional capability of the passive containment cooling is assumed lost. Therefore, one (or more) inoperable PCCS condenser loop(s) must be restored to OPERABLE status within 1 hour.

E.1

If the reactor cavity and equipment [ICS/PCCS] pool water level not within the limit specified in SR 3.6.1.7.1, the PCCS may not have sufficient heat sink capacity to support containment cooling for 72 hours. Therefore, the reactor cavity and equipment [ICS/PCCS] pool water level must be restored to within require limits within 2 hours. The 2 hour Completion Time is acceptable because it requires prompt restoration of the PCCS heat sink but allows sufficient time to attempt restoration before requiring that a reactor shutdown is initiated.

If the reactor cavity-to-equipment pool gate is installed, the PCCS heat sink capacity may be degraded. Therefore, the reactor cavity-to-equipment pool gate must be removed within 8 hours. The 8 hour Completion Time is acceptable because the PCCS retains significant heat

BASES

sink capacity even with the gate installed and 8 hours allows sufficient time to attempt restoration before requiring that a reactor shutdown is initiated.

F.1

If the Required Action and Completion Time of Conditions A, B, B, D, or E are not met, functional capability of the of the passive containment cooling is assumed lost. Therefore, the plant must be placed in a MODE in which overall plant risk is minimized. This is accomplished by placing the plant in MODE 3 within 12 hours or remaining in MODE 4. 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.

Remaining in the Applicability of the LCO is acceptable because the plant risk in MODE 3 and MODE 4 is similar to or lower than the risk in MODE 5 (Ref. 2) and because the time spent in MODE 3 to restore drywell pressure to within the specified limit will be short. Going to cold shutdown results in challenges to the shutdown heat removal systems and requires restarting the plant. However, voluntary entry into MODE 5 may be made, as it is also an acceptable low-risk state.

SURVEILLANCE REQUIREMENTS

SR 3.6.1.7.1

This SR requires periodic verification that the ICS/PCCS pool water level [in each PCCS condenser sub-compartment] is ≥ [[ ] meters ([ ] feet)].

The 24 hour Frequency for this SR is based on engineering judgment related to trending 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 highly reliable ICS/PCCS pool water level alarms will provide prompt notification of abnormal water level.

SR 3.6.1.7.2

This SR requires periodic verification that the reactor cavity-to-equipment pool gate is not installed. This SR is necessary because the reactor cavity-to-equipment pool gate, if installed, would reduce the volume of water available to each ICS/PCCS condenser sub-compartment. The 31 day Frequency is acceptable because installation of the gate is a significant change in plant status that would not occur without the cognizance of the operator.

SR 3.6.1.7.3

This SR requires periodic verification that the spectacle flanges in each PCCS vent and drain line is 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 3.6.1.7.4

This SR requires periodic verification that each equalizing valve between each ICS/PCCS pool sub-compartment is open. This SR is needed to ensure that the required volume of water is available to each condenser.

The 24 month Frequency for this SR is based on engineering judgment is acceptable because the equalizing valves between ICS/PCCS pool sub-compartments are locked open and under administrative controls.

SR 3.6.1.7.5

This SR requires periodic verification that each PCCS loop has an unobstructed path from the drywell inlet, through the condenser tubes, and out the drain pipes to the GDCS pool and out the vent pipe to the suppression pool.

The Frequency for this SR is 24 months on a STAGGERED TEST BASIS. This Frequency requires testing one of the six PCCS loops 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.

This Frequency is acceptable because [no mechanism that would result in the obstruction of the PCCS flow path has been identified] and [an

BASES

unobstructed path is verified through all six PCCS loops after the first refueling interval].

SR 3.6.1.7.6

This SR requires periodic verification that each PCCS pool subcompartment has an unobstructed path for steam release through moisture separator to the atmosphere.

The Frequency is based on engineering judgment and the simplicity of the design. This Frequency is acceptable because [no mechanism that would result in the obstruction of the flow path for steam release from the PCCS pool has been identified] and [an unobstructed path is verified through all six PCCS subcompartments after the first refueling interval].

REFERENCES

1. Section 6.2.

2. [Topical Report with Technical Justification to Support Risk-Informed End States for ESBWR Plants is under development.]

B 3.6 CONTAINMENT SYSTEMS

B 3.6.2.1 Suppression Pool Average Temperature

BASES

BACKGROUND

The suppression wetwell is a reinforced concrete pressure 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 (S/RV) 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 [309.9 kPa gauge (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 complete steam condensation of the blowdown.

b. Assure containment peak pressure and temperature are below design values.

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 the pool temperature analyses required by Reference 3).

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 assumed for the Reference 2 analyses. The limit of [46.1°C (115°F)], at which testing is terminated, is [not used in the safety analyses because DBAs are assumed not to initiate during plant testing].

BASES

Suppression pool average temperature satisfies Criteria 2 and 3 of 10 CFR 50.36(c)(2)(ii).

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. At 1% RTP, heat input is approximately equal to normal system heat losses.

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 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 based 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 trends and alarms will alert operators is 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 does not apply. This is accomplished by reducing power to < 1% RTP within 12 hours. The 12 hour Completion Time for reducing reactor 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 pool heating for testing has been exceeded. Therefore, all testing must

BASES

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 and D.2

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 verification every 30 minutes that suppression pool average temperature has not exceeded [54.4°C (130°F)] because this temperature would require immediate entry into Condition E.

The Completion Time of once per 30 minutes for verification that the limits for entry into Condition E have not been exceeded is required 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 an abnormal suppression pool temperature trends and alarms will alert operators is specified limits are exceeded.

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 reducing reactor pressure to [< 1.38 MPa gauge (200 psig)] within 12 hours. The allowed Completion Time is reasonable, based on operating experience, to reach the required plant conditions from the reactor shutdown condition in an orderly manner and without challenging plant systems. Remaining in the Applicability of the LCO (i.e., > 93.3°C (200°F) is acceptable while the plant evaluates the cause of the high suppression pool temperature and initiates appropriate actions in accordance with plant procedures.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.6.2.1.1

This SR requires verification that suppression pool average temperature in within specified limits every 24 hours. The average temperature is determined automatically by instrumentation that [takes an arithmetic average] of OPERABLE suppression pool water temperature channels.

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 15.1.

3. [NUREG-0783, “Suppression Pool Temperature Limits for BWR Containments,” November 1981].

B 3.6 CONTAINMENT SYSTEMS

B 3.6.2.2 Suppression Pool Water Level

BASES

BACKGROUND	The suppression wetwell is a reinforced concrete pressure 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 (S/RV) 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 is maintained below the design pressure for DBAs of 379 kPa gauge (55 psig). The suppression pool volume ranges between 3225 m^3 (115,000 ft^3) at the low-water-level alarm of 5.4 m (213 inches) and 3285 m^3 (117,000 ft^3) at the high-water-level alarm of 5.5 m (217 inches) 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 S/RV 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 S/RV quenchers and the main vents. The lower volume also absorbs less steam energy before heating up excessively. Therefore, a minimum pool water level is specified. If suppression pool water level is too high, it could result in excessive clearing loads from S/RV 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. Suppression pool water level satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO	This LCO requires that suppression pool water level be maintained ≥ 5.4 meters (213 inches) and ≤ 5.5 meters (217 inches) 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 S/RV 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	<u>A.1</u> 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 main vents, S/RV quenchers and PCCS vent return lines are covered even if water level is below the minimum level. Additionally, protection against overpressurization may still exists 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. <u>B.1</u> If the Required Action and Completion Time of Condition A are not met, the plant must be placed in a MODE in which overall plant risk is minimized. This is accomplished by placing the plant in MODE 3 within 12 hours or remaining in MODE 4. 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. Remaining in the Applicability of the LCO is acceptable because the plant risk in MODE 3 and MODE 4 is similar to or lower than the risk in MODE

BASES

5 (Ref. 2) and because the time spent in MODE 3 to restore drywell pressure to within the specified limit will be short. Going to cold shutdown results in challenges to the shutdown heat removal systems and requires restarting the plant. However, voluntary entry into MODE 5 may be made, as it is also an acceptable low-risk state.

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 12-hour Frequency is acceptable because highly reliable drywell pressure alarms will provide prompt notification of abnormal drywell pressure.

REFERENCES

1. Chapter [6].

2. [Topical Report with Technical Justification to Support Risk-Informed End States for ESBWR Plants is under development.]

B 3.6 CONTAINMENT SYSTEMS

B 3.6.2.3 Isolation Condenser System (ICS)/Passive Containment Cooling System (PCCS) Pool Temperature

BASES

BACKGROUND

The Isolation Condensers are designed to remove heat from the RCS following a reactor isolation incident [or LOCA]. The Passive Containment Cooling (PCC) condensers are designed to remove heat from the primary containment following a LOCA [or transient that releases heat to the containment]. The ICS/PCCS pool provides the heat sink for both the Isolation Condenser System (ICS) and Passive Containment Cooling System (PCCS) condensers. When maintained at specified levels, the ICS/PCCS pool contains sufficient water to provide at least 72 hours of reactor decay heat removal capacity without operator action.

The ICS/PCCS pool is located above and outside the containment boundary, directly above the drywell top slab. The ICS/PCCS pool is a single, large pool that includes partitioned subcompartments for each ICS condenser, each PCC condenser, and an expansion pool which includes the reactor well area and the service pool. The IC and PCC pool subcompartments are connected to the expansion pool below the water level by valves that enable full use of the collective ICS/PCCS pool water inventory independent of any ICS or PCCS condenser or subcompartment. The valves are normally locked open but can be closed to isolate a subcompartment allowing it to be emptied using a portable pump to allow maintenance.

During a LOCA or RPV isolation, subcompartment water temperature could rise to about 101°C (214°F). The steam formed will be non-radioactive and have a slight positive pressure relative to station ambient. The steam from each subcompartment collects in the common air/steam space above the subcompartments and ICS/PCCS pool. The steam is then released to the atmosphere through two large-diameter discharge vents located on opposites sides of the pool. A moisture separator is installed at the entrance to the discharge vent lines to preclude excessive moisture carryover and loss of ICS/PCCS pool water. No forced circulation equipment is required for operation of the ICS/PCCS pool.

Cooling and clean up of ICS/PCCS pool water is performed by Fuel and Auxiliary Pools Cooling System (FAPCS) (Ref. 2). During normal operation, ICS/PCCS make-up is provided from the Make-up Demineralized Water System (Ref. 1). Level is maintained using an air-operated valve in the make-up water supply line controlled by a level

BASES

transmitter in the ICS/PCCS pool. Following a LOCA, makeup water is supplied via the FAPCS connection.

APPLICABLE SAFETY ANALYSES

For the PCCS, reference 3 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 ICS/PCCS pool 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.

For the ICS, reference 4 contains the results of analyses used to predict reactor coolant system pressure and temperature following a reactor isolation incident. The intent of the analyses is to demonstrate that the heat-removal capacity of the ICS/PCCS pool is adequate to maintain the reactor coolant system conditions within design limits.

ICS/PCCS pool satisfies Criteria 2 and 3 of 10 CFR 50.36(c)(2)(ii).

LCO

This LCO requires that each ICS/PCCS pool subcompartment and the expansion pool temperature be maintained within the following limits:

a) ≤ [43.3°C (110°F)] when no testing that adds heat to the ICS/PCCS pool subcompartment is being performed, and

b) ≤ [46.1°C (115°F)] when testing that adds heat to the ICS/PCCS pool subcompartment being performed.

The ICS/PCCS pool temperature must be maintained below a maximum temperature to support the operation of the PCCS and ICS. In the event of a LOCA, the passive PCCS is required to maintain the containment peak pressure and temperature below design limits (Ref. 3) for at least 72 hours after a LOCA. In the event of a reactor isolation incident during a station blackout, the ICS must maintain the reactor coolant system pressure and temperature below design limits (Ref. 4) and remove core decay heat for at least 72 hours after reactor isolation.

Allowing a small increase in the temperature of an ICS/PCCS pool subcompartment or the expansion pool during testing that adds heat to the pool is acceptable because an increase in pool temperature results in a relatively small loss in the total heat sink capacity and significant heat sink capacity is still available.

BASES

The ICS/PCCS pool must satisfy all the performance and physical arrangement SRs in order to be considered OPERABLE.

APPLICABILITY

The ICS/PCCS pool is required to be OPERABLE in MODES 1, 2, 3, and 4 because a DBA could cause a pressurization and heat up of containment requiring the PCCS or an RPV isolation could require initiation of the ICS.

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, ICS/PCCS pool cooling is not required to be OPERABLE in MODES 5 and 6.

ACTIONS

The ACTIONS are modified by a Note that clarifies that, for this LCO, separate Condition entry is allowed for each subcompartment and the expansion pool. This is acceptable because the Required Actions for each Condition provide appropriate compensatory actions for each inoperable subcompartment or the expansion pool. Complying with the Required Actions may allow for operation to continue. This note clarifies that a subsequent inoperable subcompartment or the expansion pool is governed by same Condition and associated Required Actions used for the other subcompartment and the expansion pool.

<u>A.1</u>

If ICS/PCCS pool subcompartment or expansion pool temperature is [> 43.3°C (110°F)] when no testing that adds heat to the pool is in progress, one of the initial conditions used in the analyses in references 3 and 4 may not be met. Therefore, Required Action A.1 requires that the subcompartment and the expansion pool be restored to within the specified limit within 24 hours.

The Completion Time of 24 hours to restore the temperature to within specified limits is acceptable because a relatively small loss in the total heat sink capacity and significant heat sink capacity is still available. Therefore, continued operation is allowed for a limited time. Additionally, the 24-hour Completion Time is adequate to allow the pool temperature to be restored below the limit.

BASES

B.1 and B.2

If the Required Action and associated Completion Time of Condition A is not met, there is some degradation of the heat sink. Therefore, Required Action B.1 requires that each ICS loop and each PCCS loop affected by the high temperature in the ICS/PCCS pool must be declared inoperable within 12 hours. The Completion Time of 12 hours is acceptable because an increase in pool temperature results in a relatively small loss in the total heat sink capacity and significant heat sink capacity is still available.

Alternately, if the Required Action and associated Completion Time of Condition A is not met, Required Action B.2 requires specifies that the plant must be placed in a MODE in which overall plant risk is minimized. This is accomplished by placing the plant in MODE 3 within 12 hours or remaining in MODE 4. 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.

Remaining in the Applicability of the LCO is acceptable because the plant risk in MODE 3 and MODE 4 is similar to or lower than the risk in MODE 5 (Ref. 5) and because the time spent in MODE 3 to restore drywell pressure to within the specified limit will be short. Going to cold shutdown results in challenges to the shutdown heat removal systems and requires restarting the plant. However, voluntary entry into MODE 5 may be made, as it is also an acceptable low-risk state.

C.1

If ICS/PCCS pool subcompartment or expansion pool temperature is [> 46.1°C (115°F)] when testing that adds heat to the pool is in progress, one of the initial conditions used in the analyses in references 3 and 4 may not be met. Therefore, Required Action B.1 requires that that all testing that adds heat to the pool must be suspended immediately. When testing is suspended, Condition C is applicable.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.6.2.3.1

This SR requires verification that ICS/PCCS pool subcompartment and expansion pool temperature in within specified limits every 24 hours.

The 24 hour Frequency for this SR is based on engineering judgment related to trending pool temperature changes and the need for assessing the proximity to the specified limits. The 24 hour Frequency is acceptable because highly reliable ICS/PCCS pool subcompartment and expansion pool temperature alarms will provide prompt notification of abnormal pool temperature.

REFERENCES

1. Section [9.4].
2. Section [9.1].
3. Section [6.2].
4. Section [5.2].
5. [Topical Report with Technical Justification to Support Risk-Informed End States for ESBWR Plants is under development.]

B 3.6 CONTAINMENT SYSTEMS

B 3.6.2.4 Isolation Condenser System (ICS)/Passive Containment Cooling System (PCCS) Pool Water Level

BASES

BACKGROUND

The Isolation Condensers are designed to remove heat from the RCS following a reactor isolation incident [or LOCA]. The Passive Containment Cooling (PCC) condensers are designed to remove heat from the primary containment following a LOCA [or transient that releases heat to the containment]. The ICS/PCCS pool provides the heat sink for both the Isolation Condenser System (ICS) and Passive Containment Cooling System (PCCS) condensers. When maintained at specified levels, the ICS/PCCS pool contains sufficient water to provide at least 72 hours of reactor decay heat removal capacity without operator action.

The ICS/PCCS pool is located above and outside the containment boundary, directly above the drywell top slab. The ICS/PCCS pool is a single, large pool that includes partitioned subcompartments for each ICS condenser, each PCC condenser, [and an expansion pool which includes the reactor well area and the service pool]. The IC and PCC pool subcompartments are connected to the [main pool volume] below the water level by valves that enable full use of the collective ICS/PCCS pool water inventory independent of the status of any ICS or PCCS condenser or subcompartment. The interconnection valves are normally locked open but can be closed to isolate a subcompartment allowing it to be emptied using a portable pump. Emptying the subcompartment allows maintenance of the condenser during refueling.

During a LOCA or RPV isolation, subcompartment water temperature could rise to about 101°C (214°F). The steam formed will be non-radioactive and have a slight positive pressure relative to station ambient. The steam from each subcompartment collects in the common air/steam space above the subcompartments and ICS/PCCS pool. The steam is then released to the atmosphere through two large-diameter discharge vents located on opposites sides of the pool. A moisture separator is installed at the entrance to the discharge vent lines to preclude excessive moisture carryover and loss of ICS/PCCS pool water. No forced circulation equipment is required for operation of the ICS/PCCS pool.

Cooling and clean-up of ICS/PCCS pool water is performed by Fuel and Auxiliary Pools Cooling System (FAPCS) (Ref. 1). Suction lines, at various pool locations, draw water from the sides of the ICS/PCCS pool at an elevation above the minimum ICS/PCCS pool water level required during normal plant operation. After the water is cooled and cleaned, it is returned back to the pool.

An ICS/PCCS pool post-LOCA pool water make-up connection enters the ICS/PCCS pool via the FAPCS connection. ICS/PCCS pool clean make-up water supply for replenishing level is provided from Make-up Demineralized Water System. Level control is accomplished by using an air-operated valve in the make-up water supply line. The valve opening/closing is controlled by water level signal sent by a level transmitter sensing water level in the ICS/PCCS pool.

APPLICABLE SAFETY ANALYSES

For the PCCS, reference 2 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 ICS/PCCS pool 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.

For the ICS, reference 3 contains the results of analyses used to predict reactor coolant system pressure and temperature following a reactor isolation incident. The intent of the analyses is to demonstrate that the heat-removal capacity of the ICS/PCCS pool is adequate to maintain the reactor coolant system conditions within design limits.

ICS/PCCS pool satisfies Criteria 2 and 3 of 10 CFR 50.36(c)(2)(ii).

LCO

This LCO requires that each ICS/PCCS pool subcompartment and the expansion pool water level be maintained ≥ [4.4 meters (14.4 feet)].

The ICS/PCCS pool must be maintained above a minimum level to support the operation of the PCCS and ICS. In the event of a LOCA, the passive PCCS is required to maintain the containment peak pressure and temperature below design limits (Ref. 2) for at least 72 hours after a LOCA. In the event of a reactor isolation incident during a station blackout, the ICS must maintain the reactor coolant system pressure and temperature below design limits (Ref. 3) and remove core decay heat for at least 72 hours after reactor isolation.

APPLICABILITY

The ICS/PCCS pool is required to be OPERABLE in MODES 1, 2, 3, and 4 because a DBA could cause a pressurization and heat up of

BASES

containment requiring the PCCS or an RPV isolation could require initiation of the ICS.

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, ICS/PCCS pool cooling is not required to be OPERABLE in MODES 5 and 6.

ACTIONS

A.1

If ICS/PCCS pool water level not above the specified minimum, one of the initial conditions used in the analyses in references 3 and 4 may not be met. Therefore, Required Action A.1 requires that the pool level be restored to within the specified limit within 2 hours.

The Completion Time of 2 hours to restore the level to within specified limits is necessary because a reduced pool inventory could significantly affect heat sink capacity.

B.1

If the Required Action and associated Completion Time of Condition A is not met, Required Action B.1 requires that the plant be placed in a MODE in which overall plant risk is minimized. This is accomplished by placing the plant in MODE 3 within 12 hours or remaining in MODE 4. 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.

Remaining in the Applicability of the LCO is acceptable because the plant risk in MODE 3 and MODE 4 is similar to or lower than the risk in MODE 5 (Ref. 4) and because the time spent in MODE 3 to restore drywell pressure to within the specified limit will be short. Going to cold shutdown results in challenges to the shutdown heat removal systems and requires restarting the plant. However, voluntary entry into MODE 5 may be made, as it is also an acceptable low-risk state.

SURVEILLANCE REQUIREMENTS

SR 3.6.2.4.1

Verifying that ICS/PCCS pool level is ≥ 4.4 meters (14.4 feet) at least every 31 days ensures that the pool provides a minimum of 1100 m^3 above the top of the IC Condenser tubes and 1250 m^3 above the top of

BASES

the PCC condenser tubes. The frequency for this SR was developed based on operating experience with the slow change in pool water level due to evaporation and on additional indications available in the control room, including alarms, to alert the operator to an abnormal water level.

REFERENCES

1. Chapter 9.

2. Chapter 6.

3. Chapter 5.

4. [Topical Report with Technical Justification to Support Risk-Informed End States for ESBWR Plants is under development.]

B 3.6 CONTAINMENT SYSTEMS

B 3.6.3.1 Reactor Building

BASES

BACKGROUND

The Reactor Building (RB) is a reinforced concrete structure that completely surrounds the containment. 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 and [minimal] credit is taken for the existence of the RB surrounding the primary containment vessel in any radiological analyses. [Some] credit is taken for hold up and plate out in the Reactor Building because the building is sealed during isolation and, if AC power is available, internal recirculation is active. However, [the radiological dose consequences for LOCAs are based on an assumed containment leak rate of 0.5% per day and RB bypass leakage is assumed to equal to 100% of the containment leak rate.]

The RB structure encloses all penetrations through the containment (except for the main steam tunnel, main steam and feedwater lines). Under accident conditions, the RB is isolated to provide a hold up and plate out barrier. Therefore, containment isolation valve leakage as well as penetration leakage collects in the RB. With low leakage and stagnant conditions, the RB provides a significant volume for hold up and plate out mechanisms to enhance the basic mitigating functions provided by containment.

Leakage through the MSIVs is routed through the main steamline drain lines where large volumes and surface provide effective mechanisms to hold up and plate out the relatively low leakage flow. The feedwater lines are flooded with water that acts to seal or scrub any leakage. Leakage through the drywell head and from the PCCS and ICS condensers is scrubbed by the reactor well water and large ICS/PCCS pool of water, respectively, prior to release to the environment.

The RB HVAC system does not perform an ESF/safety-related function. However, the RB HVAC system automatically isolates upon detection of high radiation levels in the ventilation exhaust system. The RB is divided into clean and contaminated radiological zones. Under normal conditions, airflow is maintained from clean to contaminated areas and then routed via the Reactor Building HVAC system to the plant stack.

BASES

Under high radiation conditions, the air flow is rerouted to the HEPA filter train or shut down to provide a hold up and plate out 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.

APPLICABLE SAFETY ANALYSES

[The radiological dose consequences for LOCAs are based on an assumed containment leak rate of 0.5% per day and RB bypass leakage is assumed to be equal to 100% of the containment leak rate.] [However, the RB HVAC system automatically isolates upon detection of high radiation levels in the ventilation exhaust system. Therefore, [some credit may be taken for hold up and plate out in the Reactor Building because the building is sealed during isolation and, if AC power is available, internal recirculation is active.]

[Reactor building satisfies Criteria 3 of 10 CFR 50.36(c)(2)(ii).]

LCO

This LCO requires that Reactor building OPERABILITY is maintained by keeping all RB equipment hatches closed, keeping RB access doors closed, except for entry and exit, and ensuring RB ventilation dampers actuate when required.

APPLICABILITY

The RB 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 provides an added barrier to fission product release from the containment during an accident.

BASES

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 is not required to be OPERABLE in MODES 5 and 6.

ACTIONS

A.1

If the RB is inoperable, the RB must be restored to OPERABLE within 24 hours. This Completion Time is acceptable because [minimal credit is taken for the existence of the RB surrounding the primary containment vessel in any radiological analyses.]

B.1

If the Required Action and associated Completion Time of Condition A are not met, Required Action B.1 requires that the plant be placed in a MODE in which overall plant risk is minimized. This is accomplished by placing the plant in MODE 3 within 12 hours or remaining in MODE 4. 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.

Remaining in the Applicability of the LCO is acceptable because the plant risk in MODE 3 and MODE 4 is similar to or lower than the risk in MODE 5 (Ref. 2) and because the time spent in MODE 3 to restore drywell pressure to within the specified limit will be short. Going to cold shutdown results in challenges to the shutdown heat removal systems and requires restarting the plant. However, voluntary entry into MODE 5 may be made, as it is also an acceptable low-risk state.

SURVEILLANCE REQUIREMENTS

SR 3.6.3.1.1

This SR requires periodic verification that all RB equipment hatches are closed. The 31 day Frequency is acceptable because RB equipment hatches are maintained in position under administrative controls that make the likelihood of a missising or mis-positioned hatch unlikely.

SR 3.6.3.1.2

This SR requires periodic verification that one RB access door in each access opening is closed, except when open for entry and exit. The 31

BASES

day Frequency is acceptable because RB access doors are monitored and alarmed to prevent mis-positioning.

SR 3.6.3.1.3

This SR requires periodic verification that RB ventilation dampers actuate on an actual or simulated isolation signal. The 24 month Frequency is based on engineering judgment and is acceptable based on the reliability of this type of component.

REFERENCES

1. Chapter 6.

2. [Topical Report with Technical Justification to Support Risk-Informed End States for ESBWR Plants is under development.]

B 3.7 PLANT SYSTEMS

B 3.7.1 Emergency Breathing Air System (EBAS)

BASES

BACKGROUND

The EBAS provides a radiologically controlled environment from which the unit can be safely monitored following a Design Basis Accident (DBA) concurrent with a loss of all onsite and offsite AC power (station blackout (SBO)).

The safety-related function of the EBAS is to control radiation exposure by maintaining a positive pressure in the control room to prevent inleakage of contaminated air and to replenish breathing air for the operating crew. THE EBAS consists of [three] independent and redundant bottled air trains. Each train consists of multiple air bottles, pressure reducers, pressure regulators, isolation valves, relief valves, an air distribution ring and the associated ductwork. The EBAS is designed to maintain a pressurized control room for 72 hours continuous occupancy after a loss-of-coolant accident (LOCA) concurrent with an SBO, followed by 27 days continuous occupancy with the control room HVAC subsystem operating in the emergency filtration mode, without exceeding a 0.05 Sv (5 rem) whole-body dose or its equivalent to any part of the body. The EBAS is automatically initiated in the event of a main control room intake radiation - high signal concurrent with an SBO. The EBAS can also be manually actuated by the control room operator following indication of a radiological event (indicative of conditions that could result in radiation exposure to control room personnel) by isolation of the main control room. EBAS operation in maintaining a pressurized control room for controlling radiation exposure is discussed in Section 6.4 and Section 9.4.1 (Refs. 1 and 2, respectively).

APPLICABLE SAFETY ANALYSES

The ability of the EBAS to maintain a positive pressure in the control room is an explicit assumption for the safety analyses presented in Chapter 6 and Chapter 15, (Refs. 1 and 3, respectively). The EBAS is assumed to operate following a LOCA concurrent with an SBO. The radiological dose to control room personnel as a result of a LOCA is summarized in Reference 3. No single failure will cause the loss of pressurized breathable air into the control room.

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

BASES

LCO

[Three] redundant trains of the EBAS are required to be OPERABLE to ensure that at least [two are] available, assuming a single failure disables one train. Total system failure could result in exceeding 0.05 Sv (5 rem) whole-body dose or its equivalent to any part of the body to the control room operators in the event of a DBA. The EBAS is considered OPERABLE when the individual components necessary to pressurize the control room are operable in each train. A train is considered OPERABLE when:

a. Air bottles are not restricted and contain sufficient breathable air;

b. Pressure regulators, valves, ductwork and pressure gages are OPERABLE, and sufficient pressurization flow can be maintained; and

c. Control room habitability area ventilation dampers for isolation of the control room envelope are OPERABLE.

In addition, the control room envelope must be maintained, including the integrity of the walls, floors, ceilings, ductwork, and access doors.

The LCO is modified by a Note allowing the control room boundary to be opened intermittently under administrative controls. For entry and exit through doors, the administrative control of the opening is performed by the person(s) entering or exiting the area. For other openings, these controls consist of stationing a dedicated individual at the opening who is in continuous communication with the control room. This individual will have a method to rapidly close the opening when a need for control room isolation is indicated.

APPLICABILITY

In MODES 1, 2, 3, and 4 the EBAS must be OPERABLE to maintain control room pressure to control operator exposure 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 EBAS OPERABLE is not required 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), and during movement of [recently] irradiated fuel assemblies in the reactor building or fuel building [(i.e., fuel that has occupied part of a critical reactor core within the previous [ ] days)].

BASES

ACTIONS

A.1

With one EBAS train inoperable, the inoperable EBAS train must be restored to OPERABLE status within 7 days. In this Condition, the remaining OPERABLE EBAS train[s are] adequate to pressurize the control room. However, the overall reliability is reduced because a single failure in [one of] the OPERABLE train[s] could result in [partial] loss of EBAS system function. The 7-day Completion Time is based on the low probability of a DBA occurring during this time period, and the fact that the remaining train[s] can provide the required capabilities.

B.1

----------------------------------REVIEWER'S NOTE----------------------------------
Adoption of Condition B is dependent on a commitment from the licensee to have written procedures available describing compensatory measures to be taken in the event of an intentional or unintentional entry into Condition B.

If the control room boundary is inoperable in MODE 1, 2, 3, or 4, the EBAS trains cannot perform their intended functions. Actions must be taken to restore an OPERABLE control room boundary within 24 hours. During the period that the control room boundary is inoperable, appropriate compensatory measures (consistent with the intent of GDC 19) should be utilized to protect control room operators from potential hazards such as radioactive contamination, toxic chemicals, smoke, temperature and relative humidity, and physical security. Preplanned measures should be available to address these concerns for intentional and unintentional entry into the condition. The 24-hour Completion Time is reasonable based on the low probability of a DBA occurring during this time period, and the use of compensatory measures. The 24-hour Completion Time is a typically reasonable time to diagnose, plan and possibly repair, and test most problems with the control room boundary.

C.1

In MODE 1, 2, 3, or 4, if the inoperable EBAS train or control room boundary cannot be restored to OPERABLE status within the associated Completion Time, the unit must be placed in a MODE that minimizes risk. To achieve this status, the unit must be placed in MODE 3 within 12 hours or remain in MODE 4. The allowable Completion Time is reasonable, based on operating experience, to reach the required unit conditions from full power conditions in an orderly manner and without challenging unit systems.

D.1 and D.2

The Required Actions of Condition D are modified by a Note indicating that LCO 3.0.3 does not apply. If moving [recently] irradiated fuel assemblies while in MODE 1, 2, 3, or 4 the fuel movement is independent of reactor operations. Therefore, inability to suspend movement of [recently] irradiated fuel assemblies would not be a sufficient reason to require a reactor shutdown.

During movement of [recently] irradiated fuel assemblies in the reactor building or fuel building, or during OPDRVs, if the inoperable EBAS train cannot be restored to operable status within the required Completion Time, then immediately suspend activities that present a potential for releasing radioactivity that might require isolation of the control room. This places the unit in a condition that minimizes risk.

If applicable, movement of [recently] irradiated fuel assemblies in the reactor building or fuel building must be immediately suspended. Suspension of these activities shall not preclude completion of movement of component to a safe position. Also, 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.

E.1

If two [or more] EBAS trains are inoperable in MODE 1, 2, 3, or 4 for reasons other than an inoperable control room boundary (i.e., Condition B), the unit must be placed in a MODE that minimizes risk. To achieve this status, the unit must be placed in MODE 3 within 12 hours or remain in MODE 4.

F.1 and F.2

The Required Actions of Condition F have been modified by a Note that states that LCO 3.0.3 does not apply. If moving [recently] irradiated fuel while in MODE 1, 2, 3, or 4, the fuel movement is independent of reactor operations. Therefore, inability to suspend movement of [recently] irradiated fuel assemblies would not be a sufficient reason to require a reactor shutdown.

BASES

During movement of [recently] irradiated fuel assemblies in the reactor building or fuel building, or during OPDRVs, with two [or more] EBAS trains inoperable, action must be taken to immediately suspend activities that represent a potential for releasing radioactivity that might require isolation of the control room. This places the unit in a condition that minimizes risk.

If applicable, movement of [recently] irradiated fuel assemblies in the reactor building or fuel building must be immediately suspended. Suspension of these activities shall not preclude completion of movement of a component to a safe position. Also, if 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 3.7.1.1

This SR verifies that each required EBAS train contains sufficient air such that [two] train[s] of EBAS will maintain the control room at the design overpressure for 72 hours. The EBAS is designed to maintain the design overpressure in the control room habitability area in the isolation mode using a total volume of [12,312,000] liters ([434,800] cubic feet) of air at Standard atmospheric temperature and pressure. The 24-hour Frequency is based on engineering judgment.

SR 3.7.1.2

This SR verifies the correct alignment for manual, power operated, and automatic valves in the EBAS flowpath to ensure that the proper flowpath exists for EBAS automatic operation. This SR does not apply to valves that are locked, sealed, or otherwise secured in position since these valves were verified to be in the correct position prior to locking, sealing, or securing. A valve that receives an initiation signal is allowed to be in a nonaccident position provided the valve will automatically reposition. This SR does not require any testing or valve manipulation; rather, it involves verification that those valves potentially capable of being mispositioned are in the correct position. This SR does not apply to valves that cannot be inadvertently misaligned, such as check valves. The 31-day Frequency is appropriate because the valves are operated under procedural control and the probability of their being mispositioned during his time period is low.

BASES

SR 3.7.1.3

This SR verifies that each control room habitability area isolation damper actuates on an actual or simulated initiation signal. The LOGIC SYSTEM FUNCTIONAL TEST in SR 3.3.5.1.5 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 3.7.1.4

This SR demonstrates the integrity of the control room enclosure and the assumed inleakage rates of potentially contaminated air. The control room positive pressure, with respect to potentially contaminated adjacent areas, is periodically tested to verify proper function of the EBAS. During the emergency mode of operation, the EBAS is designed to slightly pressurize the control room to [31] Pa ([1/8] inch water) gauge positive pressure with respect to adjacent areas to prevent unfiltered inleakage. The EBAS is designed to maintain this positive pressure at a flow rate of [47.5] L/s ([100.6] cfm) to the control room habitability area in the isolation mode. The Frequency of 60 months is based on engineering judgment.

REFERENCES

1. Section 6.4.
2. Section 9.4.1.
3. Section 15.4.

B 3.7 PLANT SYSTEMS

B 3.7.2 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 a gross failure in the Main Condenser Offgas System that results in the rupture of the Main Condenser Offgas System pressure boundary. 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 is 1 mSv (0.1 rem) TEDE, based on 10 CFR 20.1301(a)(i) (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/Mwt-second after decay of 30 minutes. The LCO is established consistent with this requirement ([4500] Mwt x 100 μCi/Mwt-second = [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 and B.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.

SURVEILLANCE REQUIREMENTS

SR 3.7.2.1

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.

BASES

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.
2. Section 15.0.
3. 10 CFR 20.1301(a)(i).

B 3.7 PLANT SYSTEMS

B 3.7.3 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 two trains, each with two three-valve chests 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 twelve turbine bypass valves (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 Section 7.7.4 (Ref. 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 triplicated 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 servo 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. 1). No credible single failure in the control system results in a minimum demand to all TCVs and TBVs. When the TBVs open, the steam flows from the bypass chest, through connecting piping, to the pressure breakdown assemblies where a series of orifices are used to further reduce the steam pressure before the steam enters the condenser.

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, and closure of one MSIV)]. 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. 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 Safety Limit MCPR 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. 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. 2).
APPLICABILITY	The Main Turbine Bypass System is required to be OPERABLE at ≥ [25%] RTP to ensure that the MCPR safety limit 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

If two trains of the Main Turbine Bypass System are inoperable (one or more TBVs inoperable on each train), or one train of the Main Turbine Bypass System is inoperable (one or more TBVs inoperable in one train) and the MCPR limits for one inoperable Main Turbine Bypass System train, 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 required Main Turbine Bypass System trains 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 3.7.3.1

Cycling each TBV through one complete cycle of full travel demonstrates that the valves are mechanically OPERABLE and will function when required. The 92-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.

SR 3.7.3.2

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

BASES

because of the potential for an unplanned transient if the Surveillance were performed with the reactor at power. From operating experience it is believed that the 24-month Frequency, which is based on the refueling cycle, is acceptable from a reliability standpoint.

SR 3.7.3.3

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 Chapter 15 (Ref. 3). 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. From operating experience it is believed that the 24-month Frequency, which is based on the refueling cycle, is acceptable from a reliability standpoint.

REFERENCES

1. Chapter 7.7.4.

2. Chapter 5.2.2.

3. Chapter 15.

B 3.7 PLANT SYSTEMS

B 3.7.4 Fuel Pool Water Level

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 meets the assumptions of iodine decontamination factors following a fuel handling accident. 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) as required by 10 CFR 50.67 (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 [4] 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 or fuel 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. The fuel pool water level satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO	The specified water level preserves the assumption of the fuel handling accident analysis (Ref. 2). As such, it is the minimum required for fuel movement within the spent fuel storage pool.
APPLICABILITY	This LCO applies whenever movement of irradiated fuel assemblies occurs in the associated fuel storage racks since the potential for a release of fission-products exists.
ACTIONS	<u>A.1</u> 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. Required Action A.1 has 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. Therefore, inability to suspend movement of irradiated fuel assemblies is not a sufficient reason to require a reactor shutdown.
SURVEILLANCE REQUIREMENTS	<u>SR 3.7.4.1</u> This SR verifies sufficient water is available to mitigate the consequences of a fuel handling accident in the spent fuel storage pool. The water level in the spent fuel storage 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 in the spent fuel storage pools is at equilibrium with the level maintained above the top of the reactor pressure vessel (RPV) flange, and the level above the top of the RPV flange is verified every 24 hours in accordance with SR 3.9.6.1.

BASES

REFERENCES	1.	Section 9.1.2.
	2.	Section 15.4.
	3.	10 CFR 50.67.
	4.	Regulatory Guide 1.183, July 2000.

B 3.8 ELECTRICAL POWER SYSTEMS

B 3.8.1 24-hour DC Sources - Operating

BASES

BACKGROUND

The station DC electrical power system supplies normal and emergency DC power for station emergency auxiliaries and for control and switching during all modes of operation. The DC electrical power system is designed to have sufficient independence, redundancy, and testability to perform its safety functions, assuming a single failure. The DC electrical power system also conforms to the recommendations of Regulatory Guide 1.6 (Ref. 1) and IEEE-308 (Ref. 2).

The 250 V DC electrical power system includes four independent 24-hour Class 1E DC electrical power subsystems (Divisions 1, 2, 3, and 4). Each 24-hour 250 V DC electrical power subsystem consists of a 250 V DC battery, a normal and standby battery charger and main distribution panel, a ground detection panel, and all the associated control equipment and interconnecting cabling.

The 480 V AC power supplies for the divisional battery chargers are from the individual Isolation Power Centers to which the particular 24-hour 250 V DC electrical power subsystem belongs. These Isolation Power Centers are fed directly from the plant investment protection (PIP) nonsafety-related buses, which are backed up by the standby diesel generators. In addition, these Isolation Power Centers have a hard-wired connection to a terminal box where a portable emergency generator may be connected in the event that power is not available from the PIP buses. In this way, separation between the independent systems is maintained and the AC power provided to the chargers can be from either preferred or standby AC power sources.

During normal operation, the standby battery charger is used to equalize its associated battery off-line, while the normal charger associated with that battery is utilized to provide power to its associated DC distribution bus. Standby chargers are supplied from the same Isolation Power Center as the normal charger. In case of loss of normal power to the battery chargers, the DC loads are automatically powered from the associated batteries.

Each of the Division 1 through 4 24-hour Class 1E DC electrical power subsystems provides power to its associated DC distribution bus, which feeds the local DC distribution panels, uninterruptible power supply (UPS) inverter, and DC motor control center.

BASES

The DC power distribution system is described in more detail in Bases for Specifications 3.8.7, “Distribution Systems - Operating,” and 3.8.8, “Distribution Systems - Shutdown.”

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 subsystem does not cause a failure in a redundant subsystem. There is no sharing between redundant Class 1E subsystems such as batteries, battery chargers, or distribution panels. Each 250 V DC battery is separately housed in a ventilated room apart from its charger, distribution, and ground detection panels. Equipment of each Division of the DC distribution system is located in an area separated physically from the other divisions. All the components of Class 1E 250 V DC subsystems are housed in Seismic Category I structures.

The 24-hour 250 V DC Class 1E batteries have sufficient stored capacity without their chargers to independently supply the safety-related loads continuously for 24 hours. Each distribution circuit is capable of transmitting sufficient energy to start and operate all required loads in that circuit. 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). The battery banks are designed to permit the replacement of individual cells.

The normal charger associated with each 24-hour 250 V DC Class 1E battery is utilized to provide power to its associated DC distribution bus, while the standby battery charger is used to equalize its associated battery off-line. Either battery charger is capable of recharging its battery from the design minimum charge to 95% of fully charged condition within 12 hours (Ref. 4).

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 electrical power system provides normal and emergency DC electrical power for the ESF systems, emergency auxiliaries, and control and switching during all MODES of operation.

The OPERABILITY of the 24-hour Class 1E DC electrical power subsystems is consistent with the initial assumptions of the accident analyses and is based upon meeting the design basis of the unit. This

BASES

includes maintaining [at least three Divisions of] 24-hour DC sources 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 24-hour DC Sources satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

The 24-hour DC Sources Divisions, each Division consisting of a battery bank, two battery chargers, and the corresponding control equipment and interconnecting cabling within the Division, 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 a 24-hour DC Sources Division does not prevent the minimum safety function from being performed (Ref 4).

APPLICABILITY

The 24-hour 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 3.8.3, "24-hour DC Sources- Shutdown."

ACTIONS

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

Condition A represents one Division with one required battery charger inoperable (e.g., the voltage limit of SR 3.8.1.1 is not maintained). The ACTIONS provide a tiered response that focuses on returning the battery to the fully charged state and restoring a fully qualified charger to OPERABLE status in a reasonable time period. Required Action A.1 requires that the battery terminal voltage be restored to greater than or equal to the minimum established float voltage within 2 hours. This time provides for returning the inoperable charger to OPERABLE status or providing an alternate means of restoring battery terminal voltage to greater than or equal to the minimum established float voltage. Restoring the battery terminal voltage to greater than or equal to the minimum established float voltage provides good assurance that, within 12 hours, the battery will be restored to its fully charged condition (Required Action A.2) from any discharge that might have occurred due to the charger inoperability.

A discharged battery having terminal voltage of at least the minimum established float voltage indicates that the battery is on the exponential charging current portion (the second part) of its recharge cycle. The time to return a battery to its fully charged state under this condition is simply a function of the amount of the previous discharge and the recharge characteristic of the battery. Thus there is good assurance of fully recharging the battery within 12 hours, avoiding a premature shutdown with its own attendant risk.

If established battery terminal float voltage cannot be restored to greater than or equal to the minimum established float voltage within 2 hours, and the charger is not operating in the current-limiting mode, a faulty charger is indicated. A faulty charger that is incapable of maintaining established battery terminal float voltage does not provide assurance that it can revert to and operate properly in the current limit mode that is necessary during the recovery period following a battery discharge event that the DC system is designed for.

If the charger is operating in the current limit mode after 2 hours that is an indication that the battery is partially discharged and its capacity margins will be reduced. The time to return the battery to its fully charged condition in this case is a function of the battery charger capacity, the amount of loads on the associated DC system, the amount of the previous discharge, and the recharge characteristic of the battery. The charge time can be extensive, and there is not adequate assurance that it can be recharged within 12 hours (Required Action A.2).

Required Action A.2 requires that the battery float current be verified as less than or equal to [2] amps. This indicates that, if the battery had been discharged as the result of the inoperable battery charger, it has now been fully recharged. If at the expiration of the initial 12 hour period the battery float current is not less than or equal to [2] amps this indicates there may be additional battery problems and the battery must be declared inoperable.

Required Action A.3 limits the restoration time for the inoperable battery charger to 7 days. This action is applicable if an alternate means of restoring battery terminal voltage to greater than or equal to the minimum established float voltage has been used. The 7-day Completion Time reflects a reasonable time to effect restoration of the qualified battery charger to OPERABLE status.

B.1

Condition B represents one Division with one battery inoperable. With one battery inoperable, the OPERABLE battery charger is supplying the DC bus. Any event that results in a loss of the AC bus supporting the battery charger will also result in loss of DC to that Division. However, recovery of the AC bus is independent of the inoperable battery. In addition, the battery chargers have the capability of operating as battery eliminators. The battery eliminator feature is incorporated as a precautionary measure to protect against the effects of inadvertent disconnection of the battery. The battery chargers are designed to function properly and remain stable on the disconnection of the battery. The 48-hour limit allows sufficient time to effect restoration of an inoperable battery given that the majority of the conditions that lead to battery inoperability (e.g., loss of battery charger, battery cell voltage less than [2.07] V, etc.) are identified in Specifications 3.8.1, 3.8.3, and 3.8.4 together with additional specific completion times.

C.1

Condition C represents one Division with a loss of ability to completely respond to an event, and a potential loss of ability to remain energized during normal operation. It is, therefore, imperative that the operator's attention focuses on stabilizing the unit, minimizing the potential for complete loss of DC power to the affected division. The 2 hour limit is consistent with the allowed time for an inoperable DC distribution system division.

If one of the required divisional DC electrical power subsystems is inoperable for reasons other than Condition A or B (e.g., inoperable battery charger and associated inoperable battery), the remaining DC electrical power subsystems have the capacity to support a safe shutdown and to mitigate an accident condition. Since a subsequent worst-case single failure could, however, result in the loss of minimum necessary DC electrical subsystems, continued power operation should not exceed 2 hours. The 2-hour Completion Time is based on Regulatory Guide 1.93 (Ref. 7) and reflects a reasonable time to assess unit status as a function of the inoperable DC electrical power subsystem and, if the DC electrical power subsystem is not restored to OPERABLE status, to prepare to effect an orderly and safe unit shutdown.

D.1 and D.2

If a single inoperable DC electrical power subsystem cannot be restored to OPERABLE status within the associated Completion Time, the unit must be placed in a MODE that minimizes risk. To achieve this status, the unit must be placed in at least MODE 3 within 12 hours. The Completion Time is reasonable, based on operating experience related to the amount of time required to reach the required MODE 3 from full power in an orderly manner and without challenging plant systems.

In addition, when two or more of the required divisional DC electrical power subsystems are inoperable, 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 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. The Completion Time to bring the unit to MODE 5 is consistent with the time required in Regulatory Guide 1.93 (Ref. 7).

SURVEILLANCE REQUIREMENTS

SR 3.8.1.1

Verifying battery terminal voltage while on float charge helps to ensure the effectiveness of the battery chargers, which support the ability of the batteries to perform their intended function. Float charge is the condition in which the charger is supplying the continuous charge required to overcome the internal losses of a battery and maintain the battery in a fully charged state while supplying the continuous steady state loads of the associated DC subsystem. On float charge, battery cells will receive adequate current to optimally charge the battery. The voltage requirements are based on the nominal design voltage of the battery and are consistent with the minimum float voltage established by the battery manufacturer ([2.20] Vpc or [264] V at the battery terminals). This voltage maintains the battery plates in a condition that supports maintaining the grid life (expected to be approximately 20 years). The 7 day Frequency is consistent with manufacturer recommendations and IEEE-450 (Ref. 8).

SR 3.8.1.2

This SR verifies the design capacity of the battery chargers. According to Regulatory Guide 1.32 (Ref. 9), the battery charger supply is recommended to be based on the largest combined demands of the various steady state loads and the charging capacity to restore the battery from the design minimum charge state to the fully charged state, irrespective of the status of the unit during these demand occurrences. The minimum required amperes and duration ensures that these requirements can be satisfied.

This SR provides two options. One option requires that each battery charger be capable of supplying [300 or 350] 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.

The other option requires that each battery charger be capable of recharging the battery after a service test coincident with supplying the largest coincident demands of the various continuous steady state loads (irrespective of the status of the plant during which these demands occur). This level of loading may not normally be available following the battery service test and will need to be supplemented with additional loads. The duration for this test may be longer than the charger sizing criteria since the battery recharge is affected by float voltage, temperature, and the exponential decay in charging current. The battery is recharged when the measured charging current is ≤ [2] amps.

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 DC electrical power system. The discharge rate and test length corresponds to the design duty cycle requirements as specified in Reference 4.

Regulatory Guide 1.129 (Ref. 10) states that the battery-service test should be performed during an outage. The Surveillance Frequency of 24 months is consistent with the recommendations of Regulatory Guide 1.32 (Ref. 9).

A Note to SR 3.8.1.3 allows the once-per-60-months performance of SR 3.8.4.6 in lieu of SR 3.8.1.3. This substitution is acceptable because SR 3.8.4.6 represents a more severe test of battery capacity than SR 3.8.1.3.

BASES

[SR 3.8.1.4

This SR requires a CHANNEL CALIBRATION or a System Functional Test of the Division 1 and 2 24-hour normal and standby battery chargers. The reason for this Surveillance is to verify the capability of operating the battery chargers as battery eliminators with the batteries disconnected. This Surveillance ensures that the battery eliminator function can be performed by verifying that the battery chargers function properly and remain stable on the disconnection of the battery. The 24-month Frequency is based on engineering judgment.]

REFERENCES

1. Regulatory Guide 1.6, March 10, 1971.
2. IEEE Standard 308, 1978.
3. IEEE Standard 485.
4. Section 8.3.2.
5. Chapter 6.
6. Chapter 15.
7. Regulatory Guide 1.93, December 1974.
8. IEEE Standard 450, [2003].
9. Regulatory Guide 1.32, February 1977.
10. Regulatory Guide 1.129, February 1978.

B 3.8 ELECTRICAL POWER SYSTEMS

B 3.8.2 72-hour DC Sources - Operating

BASES

BACKGROUND

The station DC electrical power system supplies normal and emergency DC power for station emergency auxiliaries and for control and switching during all modes of operation. The DC electrical power system is designed to have sufficient independence, redundancy, and testability to perform its safety functions, assuming a single failure. The DC electrical power system also conforms to the recommendations of Regulatory Guide 1.6 (Ref. 1) and IEEE-308 (Ref. 2).

The 250 V DC electrical power system includes two independent 72-hour Class 1E DC electrical power subsystems (Divisions 1 and 2). Each 72-hour 250 V DC electrical power subsystem consists of a 250 V DC battery, a normal and standby battery charger and main distribution panel, a ground detection panel, and all the associated control equipment and interconnecting cabling.

The 480 V AC power supplies for the divisional battery chargers are from the individual Isolation Power Centers to which the particular 24-hour 250 V DC electrical power subsystem belongs. These Isolation Power Centers are fed directly from the plant investment protection (PIP) nonsafety-related buses, which are backed up by the standby diesel generators. In addition, these Isolation Power Centers have a hard-wired connection to a terminal box where a portable emergency generator may be connected in the event that power is not available from the PIP buses. In this way, separation between the independent systems is maintained and the AC power provided to the chargers can be from either preferred or standby AC power sources.

During normal operation, the standby battery charger is used to equalize its associated battery off-line, while the normal charger associated with that battery is utilized to provide power to its associated DC distribution bus. Standby chargers are supplied from the same Isolation Power Center as the normal charger. In case of loss of normal power to the battery chargers, the DC loads are automatically powered from the associated batteries.

Each of the Division 1 and 2 72-hour Class 1E DC electrical power subsystems provides power to its associated DC distribution bus, which feeds the local DC distribution panels and uninterruptible power supply (UPS) inverter.

BASES

The 72-hour Class 1E DC power distribution system is described in more detail in Bases for Specifications 3.8.7, “Distribution Systems – Operating.”

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 subsystem does not cause a failure in a redundant subsystem. There is no sharing between redundant Class 1E subsystems such as batteries, battery chargers, or distribution panels. Each 250 V DC battery is separately housed in a ventilated room apart from its charger, distribution, and ground detection panels. Equipment of each Division of the DC distribution system is located in an area separated physically from the other divisions. All the components of Class 1E 250 V DC subsystems are housed in Seismic Category I structures.

The 72-hour 250 V DC Class 1E batteries have sufficient stored capacity without their chargers to independently supply the safety-related loads continuously for 72 hours. Each distribution circuit is capable of transmitting sufficient energy to start and operate all required loads in that circuit. 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). The battery banks are designed to permit the replacement of individual cells without loss of availability or capability.

The normal charger associated with each 72-hour 250 V DC Class 1E battery is utilized to provide power to its associated DC distribution bus, while the standby battery charger is used to equalize its associated battery off-line. Either battery charger is capable of recharging its battery from the design minimum charge to 95% of fully charged condition within 12 hours (Ref. 4).

APPLICABLE SAFETY ANALYSES

The 72-hour Class 1E DC electrical power subsystems provide power to Post-Accident Monitoring Instrumentation required OPERABLE in MODES 1 and 2 as described in LCO 3.3.3.1, “Post-Accident Monitoring (PAM) Instrumentation.” The primary purpose of the PAM Instrumentation is to display plant variables that provide information required by the control room operators during accident situations. This information provides the necessary support for the operator to take the manual actions for which no automatic control is provided and that are required for safety systems to accomplish their safety functions for design basis events.

BASES

The 72-hour DC Sources satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

The 72-hour DC Sources Divisions, each Division consisting of a battery bank, two battery chargers, and the corresponding control equipment and interconnecting cabling within the Division, are required to be OPERABLE to ensure OPERABILITY of the associated PAM Instrumentation as described in LCO 3.3.3.1 to ensure the operators are 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. Loss of a 72-hour DC Sources Division does not prevent the minimum safety function from being performed (Ref 4).

APPLICABILITY

The 72-hour DC Sources are required to be OPERABLE in MODES 1 and 2 to support OPERABILITY of the associated PAM Instrumentation as described in LCO 3.3.3.1.

ACTIONS

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

Condition A represents one Division with one required battery charger inoperable (e.g., the voltage limit of SR 3.8.2.1 is not maintained). The ACTIONS provide a tiered response that focuses on returning the battery to the fully charged state and restoring a fully qualified charger to OPERABLE status in a reasonable time period. Required Action A.1 requires that the battery terminal voltage be restored to greater than or equal to the minimum established float voltage within 2 hours. This time provides for returning the inoperable charger to OPERABLE status or providing an alternate means of restoring battery terminal voltage to greater than or equal to the minimum established float voltage. Restoring the battery terminal voltage to greater than or equal to the minimum established float voltage provides good assurance that, within 12 hours, the battery will be restored to its fully charged condition (Required Action A.2) from any discharge that might have occurred due to the charger inoperability.

A discharged battery having terminal voltage of at least the minimum established float voltage indicates that the battery is on the exponential charging current portion (the second part) of its recharge cycle. The time to return a battery to its fully charged state under this condition is simply a function of the amount of the previous discharge and the recharge characteristic of the battery. Thus there is good assurance of fully recharging the battery within 12 hours, avoiding a premature shutdown with its own attendant risk.

If established battery terminal float voltage cannot be restored to greater than or equal to the minimum established float voltage within 2 hours, and the charger is not operating in the current-limiting mode, a faulty charger is indicated. A faulty charger that is incapable of maintaining established battery terminal float voltage does not provide assurance that it can revert to and operate properly in the current limit mode that is necessary during the recovery period following a battery discharge event that the DC system is designed for.

If the charger is operating in the current limit mode after 2 hours that is an indication that the battery is partially discharged and its capacity margins will be reduced. The time to return the battery to its fully charged condition in this case is a function of the battery charger capacity, the amount of loads on the associated DC system, the amount of the previous discharge, and the recharge characteristic of the battery. The charge time can be extensive, and there is not adequate assurance that it can be recharged within 12 hours (Required Action A.2).

Required Action A.2 requires that the battery float current be verified as less than or equal to [2] amps. This indicates that, if the battery had been discharged as the result of the inoperable battery charger, it has now been fully recharged. If at the expiration of the initial 12 hour period the battery float current is not less than or equal to [2] amps this indicates there may be additional battery problems and the battery must be declared inoperable.

Required Action A.3 limits the restoration time for the inoperable battery charger to 7 days. This action is applicable if an alternate means of restoring battery terminal voltage to greater than or equal to the minimum established float voltage has been used. The 7-day Completion Time reflects a reasonable time to effect restoration of the qualified battery charger to OPERABLE status.

B.1

Condition B represents one Division inoperable. With one Division inoperable, the remaining OPERABLE Division is capable of supplying emergency power for the minimum required PAM Instrumentation. In addition, both Divisions of the 72-hour Class 1E DC power distribution system are likely to remain energized from the other non-emergency sources depending on the nature of the inoperability. The 30-day Completion Time is based on operating experience and takes into account the remaining OPERABLE Division, the probability that the inoperable Division of the 72-hour Class 1E DC power distribution system is likely to remain energized from the other non-emergency sources, the

BASES

passive nature of the PAM Instrumentation (no critical automatic action is assumed to occur from these instruments), and the low probability of an event requiring PAM Instrumentation during this interval.

C.1

Condition C represents both Divisions inoperable. With both Divisions inoperable, emergency power for the minimum required PAM Instrumentation is not available. However, both Divisions of the 72-hour Class 1E DC power distribution system are likely to remain energized from the other non-emergency sources depending on the nature of the inoperability. The Completion Time of 7 days to restore one Division to OPERABLE status is based on the relatively low probability of an event requiring PAM Instrumentation, the probability that the inoperable Divisions of the 72-hour Class 1E DC power distribution system are likely to remain energized from the other non-emergency sources, and the availability of alternate means to obtain similar information from non-PAM Instrumentation. Continuous operation with both Divisions inoperable is not acceptable because the alternate indications are not likely to be provided with an emergency power source.

D.1

If the inoperable 72-hour DC Sources Division(s) cannot be restored to OPERABLE status within the associated Completion Times, the unit 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 Completion Time is reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.8.2.1

Verifying battery terminal voltage while on float charge helps to ensure the effectiveness of the battery chargers, which support the ability of the batteries to perform their intended function. Float charge is the condition in which the charger is supplying the continuous charge required to overcome the internal losses of a battery and maintain the battery in a fully charged state while supplying the continuous steady state loads of the associated DC subsystem. On float charge, battery cells will receive adequate current to optimally charge the battery. The voltage requirements are based on the nominal design voltage of the battery and are consistent with the minimum float voltage established by the battery manufacturer ([2.20] V per cell or [264] V at the battery terminals). This voltage maintains the battery plates in a condition that supports maintaining the grid life (expected to be approximately 20 years). The 7 day Frequency is consistent with manufacturer recommendations and IEEE-450 (Ref. 5).

SR 3.8.2.2

This SR verifies the design capacity of the battery chargers. According to Regulatory Guide 1.32 (Ref. 6), the battery charger supply is recommended to be based on the largest combined demands of the various steady state loads and the charging capacity to restore the battery from the design minimum charge state to the fully charged state, irrespective of the status of the unit during these demand occurrences. The minimum required amperes and duration ensures that these requirements can be satisfied.

This SR provides two options. One option requires that each battery charger be capable of supplying [250 or 350] 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.

The other option requires that each battery charger be capable of recharging the battery after a service test coincident with supplying the largest coincident demands of the various continuous steady state loads (irrespective of the status of the plant during which these demands occur). This level of loading may not normally be available following the battery service test and will need to be supplemented with additional loads. The duration for this test may be longer than the charger sizing criteria since the battery recharge is affected by float voltage, temperature, and the exponential decay in charging current. The battery is recharged when the measured charging current is $\leq$ [2] amps.

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.

SR 3.8.2.3

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 DC electrical

BASES

power system. The discharge rate and test length corresponds to the design duty cycle requirements as specified in Reference 4.

Regulatory Guide 1.129 (Ref. 7) states that the battery-service test should be performed during an outage. The Surveillance Frequency of 24 months is consistent with the recommendations of Regulatory Guide 1.32 (Ref. 6).

A Note to SR 3.8.2.3 allows the once-per-60-months performance of SR 3.8.4.6 in lieu of SR 3.8.2.3. This substitution is acceptable because SR 3.8.4.6 represents a more severe test of battery capacity than SR 3.8.2.3.

REFERENCES

1. Regulatory Guide 1.6, March 10, 1971.
2. IEEE Standard 308, 1978.
3. IEEE Standard 485.
4. Section 8.3.2.
5. IEEE Standard 450, [2003].
6. Regulatory Guide 1.32, February 1977.
7. Regulatory Guide 1.129, February 1978.

B 3.8 ELECTRICAL POWER SYSTEMS

B 3.8.3 24-hour DC Sources - Shutdown

BASES

BACKGROUND

A description of the 24-hour DC Sources is provided in the Bases for LCO 3.8.1, “24-hour 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 24-hour DC Sources provides normal and emergency DC electrical power for the ESF systems, emergency auxiliaries, and control and switching during all MODES of operation.

The OPERABILITY of the 24-hour 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 24-hour DC Sources during MODES 5 and 6 and during movement of [recently] irradiated fuel assemblies in the RB and FB 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 or a fuel handling accident [involving handling recently irradiated fuel. Due to radioactive decay, DC electrical power is only required to mitigate fuel handling accidents involving handling recently irradiated fuel (i.e., fuel that has occupied part of a critical reactor core within the previous [ ] days)].

In general, when the unit is shut down, the Technical Specifications requirements ensure that the unit has the capability to mitigate the consequences of postulated accidents. However, assuming a single failure and concurrent loss of all offsite or all onsite power is not required. The rationale for this is based on the fact that many Design Basis Accidents (DBAs) that are analyzed in MODES 1, 2, 3, and 4 have no specific analyses in MODES 5 and 6. Worst case bounding events are deemed not credible in MODES 5 and 6 because the energy contained within the reactor pressure boundary, reactor coolant temperature and pressure, and the corresponding stresses result in the probabilities of occurrence being significantly reduced or eliminated, and in minimal consequences. These deviations from DBA analysis assumptions and design requirements during shutdown conditions are allowed by the LCO for required systems.

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 24-hour DC Sources satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

The 24-hour DC Sources Divisions, each required Division consisting of a battery bank, two battery chargers, and the corresponding control equipment and interconnecting cabling within the Division, are required to be OPERABLE to support Distribution System Divisions required OPERABLE by LCO 3.8.8, "Distribution Systems - Shutdown." This ensures the availability of sufficient DC electrical power sources to operate the unit in a safe manner and to mitigate the consequences of postulated events during shutdown (e.g., fuel handling accidents [involving handling recently irradiated fuel] and inadvertent reactor vessel draindown).

APPLICABILITY

The 24-hour DC Sources Divisions required to be OPERABLE in MODES 5 and 6 and during movement of [recently] irradiated fuel assemblies in the Reactor Building (RB) or Fuel Building (FB) provide assurance that:

BASES

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 needed to mitigate a fuel handling accident [involving handling recently irradiated fuel (i.e., fuel that has occupied part of a critical reactor core within the previous [ ] days)] are available,

c. Required features necessary to mitigate the effects of events that can lead to core damage during shutdown are available, and

d. Instrumentation and control capability is available for monitoring and maintaining the unit in a cold shutdown condition or refueling condition.

The DC electrical power requirements for MODES 1, 2, 3, and 4 are addressed in the Bases for LCO 3.8.1, “24-hour DC Sources- Operating.”

ACTIONS

A.1, A.2.1, A.2.2, A.2.3, and A.2.4

If more than one Class 1E DC power distribution subsystem is required according to LCO 3.8.8, the DC power distribution subsystem(s) remaining OPERABLE with one or more 24-hour DC Source(s) inoperable may be capable of supporting sufficient systems to allow continuation of CORE ALTERATIONS, [recently] irradiated fuel movement, and/or operations with a potential for draining the reactor vessel. By allowing the option to declare systems inoperable with associated 24-hour DC Source(s) 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, movement of [recently] irradiated fuel assemblies, 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 24-hour DC Source(s) and to continue this action until restoration is accomplished in order to provide the necessary DC electrical power to the plant safety systems.

BASES

The Completion Time of immediately is consistent with the required times for actions requiring prompt attention. The restoration of the required 24-hour DC Source(s) 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 3.8.3.1

SR 3.8.3.1 requires performance of all Surveillances required by SR 3.8.1.1 through SR 3.8.1.3. Therefore, see the corresponding Bases for Specification 3.8.1 for a discussion of each SR.

REFERENCES

1. Chapter 6.

2. Chapter 15.

B 3.8 ELECTRICAL POWER SYSTEMS

B 3.8.4 Battery Parameters

BASES

BACKGROUND

This LCO delineates the limits on battery float current as well as electrolyte temperature, level, and float voltage for the DC power source batteries. A discussion of these batteries and their OPERABILITY requirements is provided in the Bases for LCO 3.8.1, "24-hour DC Sources - Operating", LCO 3.8.2, "72-hour DC Sources - Operating", and LCO 3.8.3, "24-hour DC Sources - Shutdown." In addition to the limitations of this Specification, the [Battery Monitoring and Maintenance Program] also implements a program specified in Specification [5.5.14] for monitoring various battery parameters that is based on the recommendations of IEEE Standard 450-[2003], "IEEE Recommended Practice for Maintenance, Testing, and Replacement of Vented Lead-Acid Batteries for Stationary Applications" (Ref. 1).

The battery cells are of flooded lead acid construction with a nominal specific gravity of [1.215]. This specific gravity corresponds to an open circuit battery voltage of approximately [247.8] V for [120] cell battery (i.e., cell voltage of [2.065] volts per cell (Vpc)). The open circuit voltage is the voltage maintained when there is no charging or discharging. Once fully charged with its open circuit voltage ≥ [2.065] Vpc, the battery cell will maintain its capacity for [30] days without further charging per manufacturer's instructions. Optimal long-term performance however, is obtained by maintaining a float voltage [2.20 to 2.25] Vpc. This provides adequate over-potential, which limits the formation of lead sulfate and self-discharge. The nominal float voltage of [2.22] Vpc corresponds to a total float voltage output of [266.4] V for a [120] cell battery as discussed in Chapter 8 (Ref. 2).

APPLICABLE SAFETY ANALYSES

The initial conditions of Design Basis Accident (DBA) and transient analyses in Chapter 6 (Ref. 3) and Chapter 15 (Ref. 4) assume that Engineered Safety Feature (ESF) systems are OPERABLE. The DC electrical power system provides normal and emergency DC electrical power for the ESF systems, emergency auxiliaries, and control and switching during all MODES of operation.

The OPERABILITY of the DC subsystems is consistent with the initial assumptions of the accident analyses and is based upon meeting the design basis of the unit. This includes maintaining [at least three

BASES

Divisions of] DC Sources OPERABLE during accident conditions in the event of:

a. An assumed loss of all offsite AC power and all onsite non-Class 1E AC power; and

b. A worst-case single failure.

Since battery parameters support the operation of the DC power 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 power to shut down the reactor and maintain it in a safe condition after an anticipated operational occurrence or a postulated DBA. Battery parameter limits are conservatively established, allowing continued DC electrical system function even with limits not met. Additional preventative maintenance, testing, and monitoring are performed in accordance with Specification [5.5.14, Battery Monitoring and Maintenance Program].

APPLICABILITY

The battery parameters are required solely for the support of the associated DC electrical power subsystems. Therefore, battery parameter limits are only required when the DC power source is required to be OPERABLE. Refer to Applicability discussion in Bases for LCO 3.8.1, LCO 3.8.2, and LCO 3.8.3.

ACTIONS

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

With one or more cells in one or more batteries in one division < [2.07] V, the battery cell is degraded. Within 2 hours verification of the required battery charger OPERABILITY is made by monitoring the battery terminal voltage (SR 3.8.1.1 or SR 3.8.2.1 as applicable) and of the overall battery state of charge by monitoring the battery float charge current (SR 3.8.4.1). This assures that there is still sufficient battery capacity to perform the intended function. Therefore, the affected battery is not required to be considered inoperable solely as a result of one or more cells in one or more batteries < [2.07] V, and continued operation is permitted for a limited period up to 24 hours.

Since the Required Actions only specify "perform," a failure of SR 3.8.1.1, SR 3.8.2.1, or SR 3.8.4.1 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 3.8.4.1 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.

B.1 and B.2

One battery with float > [2] amps indicates that a partial discharge of the battery capacity has occurred. This may be due to a temporary loss of a battery charger or possibly due to one or more battery cells in a low voltage condition reflecting some loss of capacity. Within 2 hours verification of the required battery charger OPERABILITY is made by monitoring the battery terminal voltage. If the terminal voltage is found to be less than the minimum established float voltage there are two possibilities, the battery charger is inoperable or is operating in the current limit mode. Condition A addresses charger inoperability. If the charger is operating in the current limit mode after 2 hours that is an indication that the battery has been substantially discharged and likely cannot perform its required design functions. The time to return the battery to its fully charged condition in this case is a function of the battery charger capacity, the amount of loads on the associated DC system, the amount of the previous discharge, and the recharge characteristic of the battery. The charge time can be extensive, and there is not adequate assurance that it can be recharged within 12 hours (Required Action B.2). The battery must therefore be declared inoperable.

If the float voltage is found to be satisfactory but there are one or more battery cells with float voltage less than [2.07] V, the associated "OR" statement in Condition F is applicable and the battery must be declared inoperable immediately. If float voltage is satisfactory and there are no cells less than [2.07] V there is good assurance that, within 12 hours, the battery will be restored to its fully charged condition (Required Action B.2) from any discharge that might have occurred due to a temporary loss of the battery charger.

A discharged battery with float voltage (the charger setpoint) across its terminals indicates that the battery is on the exponential charging current portion (the second part) of its recharge cycle. The time to return a battery to its fully charged state under this condition is simply a function of the amount of the previous discharge and the recharge characteristic of the battery. Thus there is good assurance of fully recharging the battery within 12 hours, avoiding a premature shutdown with its own attendant risk.

If the condition is due to one or more cells in a low voltage condition but still greater than [2.07] V and float voltage is found to be satisfactory, this is not indication of a substantially discharged battery and 12 hours is a reasonable time prior to declaring the battery inoperable.

Since Required Action B.1 only specifies "perform," a failure of SR 3.8.1.1 or SR 3.8.2.1 acceptance criteria does not result in the Required Action not met. However, if SR 3.8.1.1 or SR 3.8.2.1 is failed, the appropriate Condition(s), depending on the cause of the failure, is entered.

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

With one battery with one or more cells electrolyte level above the top of the plates, but below the minimum established design limits, the battery still retains sufficient capacity to perform the intended function. Therefore, the affected battery is not required to be considered inoperable solely as a result of electrolyte level not met. Within 31 days the minimum established design limits for electrolyte level must be re-established.

With electrolyte level below the top of the plates there is a potential for dryout and plate degradation. Required Actions C.1 and C.2 address this potential (as well as provisions in Specification [5.5.14, Battery Monitoring and Maintenance Program]). They are modified by a Note that indicates they are only applicable if electrolyte level is below the top of the plates. Within 8 hours level is required to be restored to above the top of the plates. The Required Action C.2 requirement to verify that there is no leakage by visual inspection and the Specification [5.5.14.b] item to initiate action to equalize and test in accordance with manufacturer's recommendation are taken from Annex D of IEEE Standard 450-[2003]. 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.

D.1

With one battery with pilot cell temperature less than the minimum established design limits, 12 hours is allowed to restore the temperature to within limits. A low electrolyte temperature limits the current and power available. Since the battery is sized with margin, while battery capacity is degraded, sufficient capacity exists to perform the intended function and the affected battery is not required to be considered inoperable solely as a result of the pilot cell temperature not met.

BASES

E.1

With two or more 24-hour batteries with battery parameters not within limits there is not sufficient assurance that battery capacity has not been affected to the degree that the batteries can still perform their required function, given that redundant batteries are involved. With redundant batteries involved this potential could result in a total loss of function on multiple systems that rely upon the batteries. The longer Completion Times specified for battery parameters on non-redundant batteries not within limits are therefore not appropriate, and the parameters must be restored to within limits on at least one Division within 2 hours.

F.1

When any battery parameter is outside the allowances of the Required Actions for Condition A, B, C, D, or E, sufficient capacity to supply the maximum expected load requirement is not assured and the corresponding battery must be declared inoperable. Additionally, discovering one battery with one or more battery cells float voltage less than [2.07] V and float current greater than [2] amps indicates that the battery capacity may not be sufficient to perform the intended functions. The battery must therefore be declared inoperable immediately.

SURVEILLANCE REQUIREMENTS

SR 3.8.4.1

Verifying battery float current while on float charge is used to determine the state of charge of the battery. Float charge is the condition in which the charger is supplying the continuous charge required to overcome the internal losses of a battery and maintain the battery in a charged state. The float current requirements are based on the float current indicative of a charged battery. Use of float current to determine the state of charge of the battery is consistent with IEEE-450 (Ref. 1). The 7-day Frequency is consistent with IEEE-450 (Ref. 1).

This SR is modified by a Note that states the float current requirement is not required to be met when battery terminal voltage is less than the minimum established float voltage of SR 3.8.4.1. When this float voltage is not maintained the Required Actions of LCO 3.8.4 ACTION A are being taken, which provide the necessary and appropriate verifications of the battery condition. Furthermore, the float current limit of [2] amps is established based on the nominal float voltage value and is not directly applicable when this voltage is not maintained.

SR 3.8.4.2 and SR 3.8.4.5

Optimal long-term battery performance is obtained by maintaining a float voltage greater than or equal to the minimum established design limits provided by the battery manufacturer, which corresponds to [270] V at the battery terminals, or [2.25] Vpc. This provides adequate over-potential, which limits the formation of lead sulfate and self-discharge, which could eventually render the battery inoperable. Float voltages in this range or less, but greater than [2.07] Vpc, are addressed in Specification [5.5.14]. SR 3.8.4.2 and SR 3.8.4.5 require verification that the cell float voltages are equal to or greater than the short-term absolute minimum voltage of [2.07] 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. 1).

SR 3.8.4.3

The limit specified for electrolyte level ensures that the plates suffer no physical damage and maintain adequate electron transfer capability. The Frequency is consistent with IEEE-450 (Ref. 1).

SR 3.8.4.4

This Surveillance verifies that the pilot cell temperature is greater than or equal to the minimum established design limit (i.e., [40]°F). Pilot cell electrolyte temperature is maintained above this temperature to assure the battery can provide the required current and voltage to meet the design requirements. Temperatures lower than assumed in battery sizing calculations act to inhibit or reduce battery capacity. The Frequency is consistent with IEEE-450 (Ref. 1).

SR 3.8.4.6

A battery performance discharge test is a test of constant current capacity of a battery, normally done in the as found condition, after having been in service, to detect any change in the capacity determined by the acceptance test. The test is intended to determine overall battery degradation due to age and usage.

Either the battery performance discharge test or the modified performance discharge test is acceptable for satisfying SR 3.8.4.6; however, only the modified performance discharge test may be used to satisfy the battery service test requirements of SR 3.8.1.3 and SR 3.8.2.3 as applicable.

A modified discharge test is a test of the battery capacity and its ability to provide a high rate, short duration load (usually the highest rate of the duty cycle). This will often confirm the battery's ability to meet the critical period of the load duty cycle, in addition to determining its percentage of rated capacity. Initial conditions for the modified performance discharge test should be identical to those specified for a service test.

It may consist of just two rates; for instance, the one minute rate for the battery or the largest current load of the duty cycle, followed by the test rate employed for the performance test, both of which envelope the duty cycle of the service test. Since the ampere-hours removed by a one minute discharge represents a very small portion of the battery capacity, the test rate can be changed to that for the performance test without compromising the results of the performance discharge test. The battery terminal voltage for the modified performance discharge test must remain above the minimum battery terminal voltage specified in the battery service test for the duration of time equal to that of the service test.

The acceptance criteria for this Surveillance are consistent with IEEE-450 (Ref. 1) and IEEE-485 (Ref. 5). These references recommend that the battery be replaced if its capacity is below 80% of the manufacturer's rating. A capacity of 80% shows that the battery rate of deterioration is increasing, even if there is ample capacity to meet the load requirements. Furthermore, the battery is sized to meet the assumed duty cycle loads when the battery design capacity reaches this [80]% limit.

The Surveillance Frequency for this test is normally 60 months. If the battery shows degradation, or if the battery has reached 85% of its expected life and capacity is < 100% of the manufacturer's rating, the Surveillance Frequency is reduced to 12 months. However, if the battery shows no degradation but has reached 85% of its expected life, the Surveillance Frequency is only reduced to 24 months for batteries that retain capacity ≥ 100% of the manufacturer's rating. Degradation is indicated, according to IEEE-450 (Ref. 1), when the battery capacity drops by more than 10% relative to its capacity on the previous performance test or when it is 10% below the manufacturer's rating. All these Frequencies are consistent with the recommendations in IEEE-450 (Ref. 1).

REFERENCES

1. IEEE Standard 450, [2003].

2. Chapter 8.

BASES

3. Chapter 6.

4. Chapter 15.

5. IEEE Standard 485, 1983.

B 3.8 ELECTRICAL POWER SYSTEMS

B 3.8.5 Inverters - Operating

BASES

BACKGROUND

The inverters are the preferred source of power for the 24-hour and 72-hour Division 1, 2, 3, and 4 AC Vital Buses because of the stability and reliability they achieve in being powered from the associated 250 VDC battery source. There is one inverter per AC Vital Bus making a total of six inverters. The function of an inverter is to convert DC electrical power to AC electrical power, thus providing an uninterruptible power source for the instrumentation and controls for the Safety System Logic and Control (SSLC), the Reactor Protection System (RPS), and other safety-related loads requiring uninterruptible power.

APPLICABLE SAFETY ANALYSES

The initial conditions of design basis transient and accident analyses in Chapter 6, “Engineered Safety Features,” (Ref. 1) and Chapter 15, “Accident Analyses,” (Ref. 2) assume Engineered Safety Feature (ESF) systems are OPERABLE. The inverters are designed to provide the required capacity, capability, redundancy, and reliability to ensure the availability of necessary power to the RPS and ESF instrumentation and controls so that the fuel, Reactor Coolant System (RCS), and containment design limits are not exceeded. These limits are discussed in more detail in the Bases for LCO 3.2, “Power Distribution Limits,” LCO 3.4, “Reactor Coolant System,” and LCO 3.6, “Containment Systems.”

The OPERABILITY of the inverters is consistent with the initial assumptions of the accident analyses and is based on meeting the design basis of the unit. This includes maintaining electrical power sources 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.

Inverters are a part of the distribution system and, as such, satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO	The inverters ensure the availability of AC electrical power for the instrumentation for the systems required to shut down the reactor and maintain it in a safe condition after an anticipated operational occurrence (AOO) or a postulated DBA. Maintaining the required inverters OPERABLE ensures that the redundancy incorporated into the design of the RPS and ESFAS instrumentation and controls is maintained. The six battery-powered inverters ensure an uninterruptible supply of AC electrical power to the AC Vital Buses even if the 480 VAC non safety-related buses are de-energized. An OPERABLE inverter requires the associated AC Vital Bus be powered by the inverter with output voltage and frequency within design tolerances, and the inverter be powered from the associated 250 VDC 24-hour or 72-hour battery.
APPLICABILITY	The inverters are required to be OPERABLE in MODES 1, 2, 3, and 4 to ensure that: a. Acceptable fuel design limits and reactor coolant pressure boundary limits are not exceeded as a result of AOOs or abnormal transients; 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 3.8.6, “Inverters – Shutdown.”
ACTIONS	The ACTIONS table is modified by a Note indicating that a separate Condition entry is allowed for one 24-hour inverter and one or two 72-hour inverters. This is acceptable, since the Required Actions for each Condition provide appropriate compensatory actions for each inoperable inverter. Complying with the Required Actions may allow for continued operation, and subsequent inoperable inverters are governed by subsequent Condition entry and application of associated Required Actions.

A.1

With one inverter inoperable the ability to respond to an event and the overall reliability of the associated Division AC Vital Bus is reduced.

With one 24-hour inverter inoperable, and a loss of function has not occurred, the remaining OPERABLE AC Vital Buses are capable of supporting the minimum safety functions necessary to shut down the reactor and maintain it in a safe shutdown condition, assuming a single failure. Required Action A.1 allows 24 hours to fix the inoperable inverter and return it to service. The 24 hour limit is based upon engineering judgment, taking into consideration the time required to repair an inverter and the additional risk to which the 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. When the AC Vital Bus is powered from its constant voltage source, it is relying upon interruptible AC electrical power sources (offsite and onsite). The uninterruptible inverter source to the AC Vital Buses is the preferred source for powering safety-related devices.

With one 72-hour inverter inoperable, the remaining OPERABLE AC Vital Bus is capable of supplying emergency power for the minimum required PAM Instrumentation. In addition, both Divisions of the 72-hour AC Vital Buses are likely to remain energized from the other non-emergency sources depending on the nature of the inoperability. The 30-day Completion Time is based on operating experience and takes into account the remaining OPERABLE Division, the probability that the inoperable Division of the 72-hour AC Vital Bus is likely to remain energized from the other non-emergency sources, the passive nature of the PAM Instrumentation (no critical automatic action is assumed to occur from these instruments), and the low probability of an event requiring PAM Instrumentation during this interval.

Required Action A.1is modified by a Note stating that applicable Conditions and Required Actions of LCO 3.8.7 must be entered with any AC Vital Bus de-energized. This Note is necessary since, with a required inverter inoperable, its associated AC Vital Bus becomes inoperable until it is re-energized from its associated inverter. LCO 3.8.7 addresses this action; however, pursuant to LCO 3.0.6, these actions would not be entered even if the AC Vital Bus were de-energized. Therefore, the ACTIONS are modified by a Note stating that ACTIONS for LCO 3.8.7 must be entered immediately. This ensures the 24-hour AC Vital Bus is re-energized within 8 hours.

BASES

B.1

With both 72-hour inverters inoperable, emergency power for the associated AC Vital Buses and consequently the minimum required PAM Instrumentation may not be available. However, both 72-hour AC Vital Buses are likely to remain energized from other non-emergency sources depending on the nature of the inoperability. The Completion Time of 7 days to restore one inverter to OPERABLE status is based on the relatively low probability of an event requiring PAM Instrumentation, the probability that the AC Vital Buses are likely to remain energized from the other non-emergency sources, and the availability of alternate means to obtain similar information from non-PAM Instrumentation. Continuous operation with both inverters inoperable is not acceptable because the alternate indications are not likely to be provided with an emergency power source.

C.1 and C.2

If two or more 24-hour inverters are inoperable or the Required Action and associated Completion Time of Condition A is not met for any inoperable inverter, then 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, as applicable, 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.

The ACTIONS are modified by a Note stating that Required Action C.2 is only applicable with two or more 24-hour inverters inoperable. Since, the Applicability excludes the 72-hour inverters in MODES 3 and 4, this Note specifically precludes the need to place the plant in MODE 5 within 36 hours for the 72-hour inverters.

SURVEILLANCE REQUIREMENTS

SR 3.8.5.1

This Surveillance verifies that the inverters are functioning properly with all required circuit breakers closed and AC Vital Buses energized from the inverter. The verification of proper voltage and frequency output ensures that the required power is readily available for safety-related devices connected to the AC Vital Buses. The 7-day Frequency takes into account the availability of redundant inverters and other indications

BASES

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 Inverters - Shutdown

BASES

BACKGROUND	A description of the inverters is provided in the Bases for Specification 3.8.5, “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, “Accident Analyses,” (Ref. 2) assume Engineered Safety Feature (ESF) systems are OPERABLE. The inverters are designed to provide the required capacity, capability, redundancy, and reliability to ensure the availability of necessary power to the RPS and ESF instrumentation and controls so that the fuel, Reactor Coolant System (RCS), and containment design limits are not exceeded.

The OPERABILITY of the inverters is consistent with the initial assumptions of the accident analyses and the requirements for the supported systems' OPERABILITY.

The OPERABILITY of the minimum inverters to each AC Vital Bus during MODES 5 and 6 and during movement of [recently] irradiated fuel assemblies in the RB or FB 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 or a fuel handling accident [involving handling recently irradiated fuel. Due to radioactive decay, the DC to AC inverters are only required to mitigate fuel handling accidents involving handling recently irradiated fuel (i.e., fuel that has occupied part of a critical reactor core within the previous [ ] days)].

In general, when the unit is shut down, the Technical Specifications requirements ensure that the unit has the capability to mitigate the consequences of postulated accidents. However, assuming a single

BASES

failure and concurrent loss of all offsite or all onsite power is not required. The rationale for this is based on the fact that many Design Basis Accidents (DBAs) that are analyzed in MODES 1, 2, 3, and 4 have no specific analyses in MODES 5 and 6. Worst case bounding events are deemed not credible in MODES 5 and 6 because the energy contained within the reactor pressure boundary, reactor coolant temperature and pressure, and the corresponding stresses result in the probabilities of occurrence being significantly reduced or eliminated, and in minimal consequences. These deviations from DBA analysis assumptions and design requirements during shutdown conditions are allowed by the LCO for required systems.

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

The Inverters ensure the availability of electrical power for the instrumentation for systems required to shutdown the reactor and maintain it in a safe condition after an anticipated operational occurrence or postulated DBA. The battery-powered Inverters provide uninterruptible supply of AC electrical power to the AC Vital Buses even if the 480 V non safety-related buses are de-energized. OPERABLE inverters require the Vital Bus be powered by the inverter via inverted DC voltage. This ensures the availability of sufficient inverter power sources to operate the plant in a safe manner and to mitigate the consequences of postulated

BASES

events during shutdown (e.g.,[fuel handling accidents involving handling recently irradiated fuel and] inadvertent reactor vessel draindown).

APPLICABILITY

The inverters required to be OPERABLE in MODES 5 and 6, and also any time during movement of [recently] irradiated fuel assemblies in the reactor building or fuel building 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. Systems needed to mitigate a fuel handling accident [involving handling recently irradiated fuel (i.e., fuel that has occupied part of a critical reactor core within the previous [ ] days)] are available;]

c. Systems necessary to mitigate the effects of events that can lead to core damage during shutdown are available; and

d. Instrumentation and control capability is available for monitoring and maintaining the unit in a cold shutdown condition or refueling condition.

Inverter requirements for MODES 1, 2, 3, and 4 are covered in LCO 3.8.5, “Inverters - Operating.”

ACTIONS

A.1, A.2.1, A.2.2, A.2.3, and A.2.4

If two divisions are required by LCO 3.8.7, “Distribution System - Shutdown”, the remaining OPERABLE inverters may be capable of supporting sufficient required feature(s) to allow continuation of CORE ALTERATIONS, [recently] irradiated fuel movement, and/or operations with a potential for draining the reactor vessel. By allowing 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, movement of [recently] irradiated fuel assemblies in the reactor building and fuel building and any activities that could potentially result in inadvertent draining of the reactor vessel.

BASES

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 or powered from a constant voltage source transformer.

SURVEILLANCE REQUIREMENTS

SR 3.8.6.1

This Surveillance verifies that the inverters are functioning properly with all required circuit breakers closed and AC vital buses energized from the inverter. The verification of proper voltage and frequency output ensures that the required power is readily available for the instrumentation of the Reactor Protection System connected to the AC Vital Buses. The 7-day Frequency takes into account the redundant capability of the inverters and other indications available in the control room that will alert the operator to inverter malfunctions.

REFERENCES

1. Chapter 6.
2. Chapter 15.

B 3.8 ELECTRICAL POWER SYSTEMS

B 3.8.7 Distribution Systems - Operating

BASES

BACKGROUND

The Class 1E DC and AC Vital Bus safety-related electrical power distribution system is divided into independent and redundant divisions (Divisions 1, 2, 3, and 4).

The Class 1E DC distribution system consists of the 24-hour 250 VDC buses (Divisions 1, 2, 3,and 4) and, the 72-hour 250 VDC buses (Divisions 1 and 2), and associated load centers, motor control centers and distribution panels.

The Class 1E AC Vital Bus distribution system consists of the 24-hour 480 VAC vital buses (Divisions 1, 2, 3, and 4) and associated load centers, transformers, motor control centers and 120/208 VAC distribution panels, and the 72-hour 120 VAC vital buses (Divisions 1 and 2),.

The list of all distribution buses is located in Table 3.8.7-1.

APPLICABLE SAFETY ANALYSES

The initial conditions of design basis transient and accident analyses in Chapter 6, “Engineering Safety Features,” (Ref. 1) and Chapter 15, “Accident Analyses,” (Ref. 2) assume ESF systems are OPERABLE. The 24-hour DC and AC Vital Bus electrical power distribution systems are designed to provide sufficient capacity, capability, redundancy, and reliability to ensure the availability of necessary power to ESF systems so that the fuel, Reactor Coolant System (RCS) and containment design limits are not exceeded. These limits are discussed in more detail in the Bases for LCO 3.2, “Power Distribution Limits,” LCO 3.4, “Reactor Coolant System,” and LCO 3.6, “Containment Systems.”

The OPERABILITY of the DC and AC Vital Bus electrical power distribution systems is consistent with the initial assumptions of the accident analyses and is based upon meeting the design basis of the plant. The Class 1E DC and AC Vital Bus electrical power distribution systems are designed so that no single failure in any division will result in conditions that prevent safe shutdown of the plant with one division out of service.

The 72-hour DC and AC Vital Bus electrical power distribution systems are designed to provide power to Post-Accident Monitoring

BASES

Instrumentation required OPERABLE in MODES 1 and 2 as described in LCO 3.3.3.1, “Post-Accident Monitoring (PAM) Instrumentation.” The primary purpose of the PAM Instrumentation is to display plant variables that provide information required by the control room operators during accident situations. This information provides the necessary support for the operator to take the manual actions for which no automatic control is provided and that are required for safety systems to accomplish their safety functions for design basis events.

The Class 1E DC and AC Vital Bus electrical power distribution systems satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

The required Class 1E DC, and AC Vital Bus power distribution subsystems listed in Table B 3.8.7-1 ensure the availability of DC and AC Vital Bus electrical power for the systems required to shut down the reactor and maintain it in a safe condition after an anticipated operational occurrence (AOO) or a postulated DBA. The Division 1, 2, 3, and 4 Class 1E DC and AC Vital Bus electrical power primary distribution subsystems are required to be OPERABLE.

Maintaining the Division 1, 2, 3, and 4 DC and AC Vital Bus electrical power distribution subsystems 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 subsystems does not prevent safe shutdown of the reactor.

OPERABLE DC electrical power distribution subsystems require the associated buses to be energized to their proper voltage from either the associated battery or charger. OPERABLE AC vital bus electrical power distribution subsystems require the associated buses to be energized to their proper voltage from the associated inverter via inverted DC voltage.

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

BASES

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 3.8.8, “Distribution Systems – Shutdown.”

ACTIONS

A.1

With one 24-hour DC or AC Vital bus or associated load center, motor control center, or distribution panel in one division inoperable, and a loss of function has not occurred, the remaining electrical power distribution subsystems are capable of supporting the minimum safety functions necessary to shut down the reactor and maintain it in a safe shutdown condition, assuming a single failure. The overall reliability is reduced, however, and the completion time of 8 hours is established to restore the subsystem to operable status.

B.1

Condition B represents one 72-hour Division inoperable. With one Division inoperable, the remaining OPERABLE Division is capable of supplying emergency power for the minimum required PAM Instrumentation. In addition, both Divisions of the 72-hour Class 1E power distribution system are likely to remain energized from the other non-emergency sources depending on the nature of the inoperability. The 30-day Completion Time is based on operating experience and takes into account the remaining OPERABLE Division, the probability that the inoperable Division of the 72-hour Class 1E power distribution system is likely to remain energized from the other non-emergency sources, the passive nature of the PAM Instrumentation (no critical automatic action is assumed to occur from these instruments), and the low probability of an event requiring PAM Instrumentation during this interval.

C.1

Condition C represents both 72-hour Divisions inoperable. With both Divisions inoperable, emergency power for the minimum required PAM Instrumentation is not available. However, both Divisions of the 72-hour Class 1E power distribution system are likely to remain energized from other non-emergency sources depending on the nature of the inoperability. The Completion Time of 7 days to restore one Division to

OPERABLE status is based on the relatively low probability of an event requiring PAM Instrumentation, the probability that the inoperable Divisions of the 72-hour Class 1E power distribution system are likely to remain energized from the other non-emergency sources, and the availability of alternate means to obtain similar information from non-PAM Instrumentation. Continuous operation with both Divisions inoperable is not acceptable because the alternate indications are not likely to be provided with an emergency power source.

D.1 and D.2

If a single inoperable DC electrical power subsystem cannot be restored to OPERABLE status within the associated Completion Time, the unit must be placed in a MODE that minimizes risk. To achieve this status, the unit must be placed in at least MODE 3 within 12 hours. The Completion Time is reasonable, based on operating experience related to the amount of time required to reach the required MODE 3 from full power in an orderly manner and without challenging plant systems.

If two or more 24-hour DC and Vital AC Bus electrical power Divisions are inoperable, 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.

Additionally if the Required Action and associated Completion Time of Condition A, B, or C is not met, then the plant must be placed in a MODE in which the overall plant risk is minimized. To achieve this status the unit must be placed in at least MODE 3 within 12 hours.

The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.8.7.1

This Surveillance verifies that the DC and Vital AC Bus electrical power distribution systems are functioning properly, with the correct circuit breaker alignment and 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 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 DC and AC Vital Bus electrical power distribution Divisions, 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 3.8.7-1 (page 1 of 1)
DC and AC Vital Bus Electrical Power Distribution Systems

TYPE	VOLTAGE	[DIVISION 1]*	[DIVISION 2]*	[DIVISION 3]*	[DIVISION 4]*
24-hour DC buses	[250 V]	[ESF Bus] [NB01]	[ESF Bus] [NB02]	[ESF Bus] [NB01]	[ESF Bus] [NB01]
24-hour AC Vital Buses	[480 V]	Load Centers [NG01]	Load Centers [NG02, NG04]	Load Centers [NG03]	Load Centers [NG014
	[480 V]	Motor Control Centers [NG01A,]	Motor Control Centers [NG02A,]	Motor Control Centers [NG03A,]	Motor Control Centers [NG04A,]
	[120/208 V]	Distribution Panels [NP01, NP03]	Distribution Panels [NP02, NP04]	Distribution Panels [NP05, NP06]	Distribution Panels [NP07, NP08]
72-hour DC buses	[250 V]	Bus [NK01]	Bus [NK02]	N/A	N/A
72-hour AC Vital Buses	[120 V]	Bus [NK03]	Bus [NK04]	N/A	N/A

B 3.8 ELECTRICAL POWER SYSTEMS

B 3.8.8 Distribution Systems - Shutdown

BASES

BACKGROUND	A description of the DC and AC Vital Bus electrical power distribution system is provided in the Bases for LCO 3.8.7, “Distribution System - Operating.”
APPLICABLE SAFETY ANALYSES	The initial conditions of design basis transient and accident analyses in Chapter 6, “Engineering Safety features,” (Ref. 1) and Chapter 15, “Accident Analyses,” (Ref. 2) assume ESF systems are OPERABLE The 24-hour DC and AC Vital Bus electrical power distribution systems are designed to provide sufficient capacity, capability, redundancy, and reliability to ensure the availability of necessary power to ESF systems so that the fuel, Reactor Coolant System (RCS) and containment design limits are not exceeded. The OPERABILITY of the DC and AC Vital Bus electrical power distribution systems is consistent with the initial assumptions of the accident analyses and the requirements for the supported systems OPERABILITY. The OPERABILITY of the minimum DC, and AC Vital Bus electrical power distribution subsystems during MODES 5 and 6, and during movement of [recently] irradiated fuel assemblies in the primary or secondary containment 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 or a fuel handling accident [involving handling recently irradiated fuel. Due to radioactive decay, AC and DC electrical power is only required to mitigate fuel handling accidents involving handling recently irradiated fuel (i.e., fuel that has occupied part of a critical reactor core within the previous [ ] days)].

BASES

The DC and AC Vital Bus electrical power distribution systems satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

Various combinations of the DC and AC Vital Bus electrical distribution system subsystems, equipment, and components are required OPERABLE by other LCOs, 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 systems, equipment, and components - both specifically addressed by their own LCOs, and implicitly required by the definition of OPERABILITY.

Maintaining these portions of the distribution system 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., fuel handling accidents [involving handling recently irradiated fuel] and inadvertent reactor vessel draindown).

APPLICABILITY

The AC and DC electrical power distribution subsystems required to be OPERABLE in MODES 5 and 6 and during movement of [recently] irradiated fuel assemblies in the Reactor Building (RB) or Fuel Building (FB) 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. Systems 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 AC Vital Bus electrical power distribution subsystem requirements for MODES 1, 2, 3, and 4 are covered in LCO 3.8.7, “Distribution Systems - Operating.”

BASES

ACTIONS

A.1, A.2.1, A.2.2, A.2.3, and A.2.4

Although redundant required features may require redundant divisions of electrical power distribution subsystems to be OPERABLE, one OPERABLE electrical power distribution Division may be capable of supporting sufficient required features to allow continuation of CORE ALTERATIONS, [recently] irradiated fuel movement, 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, movement of [recently] irradiated fuel assemblies in the reactor building and fuel building 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 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 3.8.8.1

This Surveillance verifies that the DC and AC Vital Bus 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.

BASES

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 main 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 machine has two mechanical switches that open before the machine and the fuel grapple are physically located over the reactor vessel. The main hoist has two switches that open when the hoist is loaded with fuel. The refueling interlocks use these indications to 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

The main hoist switches open at a load lighter than the weight of a single fuel assembly in water.

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.

[The refueling machine position switches activate at a point outside of the reactor core, such that, considering switch hysteresis and maximum platform momentum toward the core at the time of power loss with a fuel assembly loaded and a control rod withdrawn, the fuel is not over the core.]

Refueling Equipment Interlocks satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

To prevent criticality during refueling, the refueling interlocks ensure that fuel assemblies are not loaded with any control rod withdrawn.

To prevent these conditions from developing, the all-rods-in, the refueling machine position, and the refueling machine main hoist fuel-loaded 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.

BASES

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 MODES.

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 to 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).

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

BASES

	and their associated input status that are available to plant operations personnel.
REFERENCES	1. 10 CFR 50, Appendix A, GDC 26. 2. Section 7.6.2. 3. Section 15.4.1.

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 is permitted to be withdrawn. To enable the one-rod/rod-pair-out interlock the RC&IS GANG/SINGLE selection switch must be in “SINGLE” mode. Otherwise, it is possible to withdraw the two rods associated with the same HCU 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 Rod Control and Information System (RCIS)).

APPLICABLE SAFETY ANALYSES

The refuel position one-rod/rod-pair-out interlock is 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.

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.

Refuel Position One-Rod/Rod-Pair-Out Interlock satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO

To prevent criticality during MODE 5, the refuel position one-rod/rod-pair-out interlock ensures no more than one control rod may be withdrawn. [Both] channels of the refuel position one-rod/rod-pair-out interlock are required to be OPERABLE and the reactor mode switch must be locked in the refuel position to support the OPERABILITY of these channels.

APPLICABILITY

In MODE 5, 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)") 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.

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 refueling position one-rod/rod-pair-out interlock requires the reactor mode switch to be in Refuel. During control rod withdrawal in MODE 5, 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

BASES

the refueling 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. 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 3.9.2.1 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 7.6.2].
3. [Section 15.4.1].

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 RCIC 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 RCIC GANG/SINGLE selection status is in the GANG mode with the individual hydraulic control unit (HCU) scram test mode active, the refueling interlocks allow two control rods that are associated with the same HCU (a control rod pair) 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), [the average power range monitor (APRM) neutron flux scram (LCO 3.3.1.1)], and the control rod block instrumentation (LCO 3.3.2.1). The safety analysis of the control rod removal error during refueling (Ref. 2) assumes the functioning of the refueling interlocks and adequate

BASES

SDM. Additionally, prior to fuel reload, all control rods must be fully inserted to minimize the probability of an inadvertent criticality.

Additionally, prior to fuel reload, all control rods must be fully inserted to ensure that an inadvertent criticality does not occur.

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.

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.

BASES

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 to prevent inadvertent criticalities during refueling operations. Control rod position is derived from synchros which have an analog output. The Rod Control and Information System (RC&IS) translates the 100% insertion signal from the resolver into a discrete full-in position signal to be used as a permissive in 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 removes the all-rods-in permissive for the refueling equipment interlocks and prevents fuel loading. Also, this condition causes the refuel position one-rod/rod-pair-out interlock to not allow 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)"), [the average power range monitor (APRM) neutron flux scram (LCO 3.3.1.1)], and the control rod block instrumentation (LCO [3.3.2.1], Control Rod Block Instrumentation"). The safety analysis for the control rod withdrawal 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.

BASES

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

LCO

[One of the two] 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 at least [one] channel of 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 [channels] 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 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 0% position indication). 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 condition will be alarmed to the operator to initiate bypass of Resolver A and use Resolver B.

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 (RCIS) 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)"), [the average power range monitor (APRM) neutron flux scram (LCO 3.3.1.1)], and the control rod block instrumentation (LCO 3.3.2.1, "Control Rod Block Instrumentation"). 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.

BASES

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 ≥ [12.755 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.

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 CRD scram accumulator pressure is ≥ [12.755 MpaG (1850 psig)].

BASES

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 15.4.1.

B 3.9 REFUELING OPERATIONS

B 3.9.6 Reactor Pressure Vessel (RPV) Water Level

BASES

BACKGROUND	The movement of irradiated fuel assemblies within the RPV requires a minimum water level of [7.01] m ([23] 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 5 rem (TEDE) in the control room as required by 10 CFR 50.67 (Ref. 2) and Regulatory Guide 1.183 (Ref. 3) acceptance criteria.
APPLICABLE SAFETY ANALYSES	During movement of irradiated fuel assemblies 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 23 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 (Ref. 2). A fuel handling accident is assumed to damage all of the fuel rods in [4] fuel assemblies as discussed in Reference 1. Analysis of the fuel handling accident inside containment is described in Reference 1. With a minimum water level of 23 ft and a minimum decay time of 24 hours prior to fuel handling, the analysis and test programs demonstrate that the iodine release due to a postulated fuel handling accident is adequately captured by the water, and that offsite doses are maintained within < 0.063 Sv (6.3 rem) total effective dose equivalent (TEDE) and 5 rem in the control room as required by 10 CFR 50.67 (Ref. 2) and Regulatory Guide 1.183 (Ref. 3) acceptance criteria. 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.

BASES

APPLICABLE SAFETY ANALYSES (continued)

RPV Water Level satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

A minimum water level of [7.01] m ([23] 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 3.

APPLICABILITY

LCO 3.9.6 is applicable during movement of irradiated fuel assemblies within the RPV. The LCO minimizes the possibility of a fuel handling accident in containment that is beyond the assumptions of the safety analysis. Requirements for fuel handling accidents in the spent fuel storage pool are covered by LCO 3.7.4, "Fuel Pool Water Level."

ACTIONS

A.1

If the water level is < [7.01] m ([23] ft.)] above the top of the RPV flange, all operations involving movement of irradiated fuel assemblies within the RPV shall be suspended immediately to ensure that a fuel handling accident cannot occur. The suspension of movement of irradiated fuel shall not preclude completion of movement to a safe position.

SURVEILLANCE REQUIREMENTS

SR 3.9.6.1

Verification of a minimum water level of [7.01] m ([23] 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 containment (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.

BASES

REFERENCES	1.	Section 15.4.1.
	2.	Regulatory Guide 1.183.
	3.	10 CFR 50.67.

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 4 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). 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. Control Rod Drive (CRD) pump or [hydrostatic test] operation and a water solid RPV (except for an air bubble for pressure control) are used to achieve the necessary temperatures and pressures required for these tests. The minimum temperatures (at the required pressures) allowed for these tests are established by the RWCU/SDC System and 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 will eventually be required with minimum reactor coolant temperatures > 93.3°C (200°F). The hydrostatic test requires increasing pressure to 110% of the operating pressure of 7.067 MPaG (1025 psig) or 7.777 MPG (1128 psig) and because of the expected increase in reactor vessel fluence, the minimum allowable vessel temperature per LCO 3.4.4 is increased as shown in the Reactor Coolant System (RCS) Pressure and Temperature Limits Report.
APPLICABLE SAFETY ANALYSES	Allowing the reactor to be considered in MODE 5 during hydrostatic or leak testing, when the reactor coolant temperature is > 93.3°C (200°F), effectively provides an exception to MODE 3 and 4 requirements including OPERABILITY of primary containment and the full complement

BASES

of redundant Emergency Core Cooling Systems. Since the hydrostatic or leak 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, "Reactor Coolant Specific Activity," are minimized. In addition, the reactor building will be OPERABLE in accordance with this Special Operations LCO, and will be capable of handling any 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 OPERABLE, 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 to be OPERABLE 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 3.5.2, "ECCS – 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.

For the purposes of this test, the protection provided by normally required MODE 5 applicable LCOs, in addition to the reactor building requirements required to be met by 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 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

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

BASES

> 93.3°C (200°F) while the ASME inservice test itself requires the safety/relief valves to be gagged, preventing their OPERABILITY.

If it is desired to perform these tests while complying with this Special Operations LCO, then the MODE 5 applicable LCOs and specified MODE 3 LCOs 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 LCOs to be met will provide sufficient protection for operations at reactor coolant temperatures > 93.3°C (200°F) for the purposes of performing either an inservice leak or hydrostatic test.

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 the 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 OPERABILITY per the imposed MODE 3 requirements 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

A.1

If an LCO specified in LCO 3.10.1 is not met, the ACTIONS applicable to the stated requirements shall be entered immediately and complied with. Required Action A.1 has been modified by a Note that clarifies the intent of another LCO's Required Action to be in MODE 5 as including reducing the average reactor coolant temperature to ≤ 93.3°C (200°F).

A.2.1 and A.2.2

Required Action A.2.1 and Required Action A.2.2 are alternate ACTIONS that can be taken instead of Required Action A.1 and are provided to 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.2.1 and the reactor coolant temperature is reduced to establish normal MODE 5 requirements. The allowed Completion Time of 24 hours for Required Action A.2.2 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

The LCOs made applicable are required to have their Surveillances met to establish that this LCO is being met.

REFERENCES

1. ASME Boiler and Pressure Vessel Code, Section XI, “Rules for Inservice Inspection of Nuclear Power Plant Components.”

2. Section 15.1.

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, multiposition, keylock switch provided to select the necessary scram functions for various plant conditions (Ref. 1). The reactor mode switch selects the appropriate trip relays for scram functions and provides appropriate bypasses. The mode switch positions and related scram interlock functions are summarized as follows: a. SHUTDOWN - Initiates a reactor scram; bypasses main steam line isolation and reactor high water level scrams; b. REFUEL - Selects Neutron Monitoring System (NMS) scram function for low neutron flux level operation (but does not disable the average power range monitor scram); bypasses main steam line isolation and reactor high water level scrams; c. STARTUP OR HOT STANDBY - Selects NMS scram function for low neutron flux level operation (startup range neutron monitors); bypasses main steam line isolation and reactor high water level scrams; and d. RUN - Selects NMS scram function for power range operation. The reactor mode switch also provides interlocks for such functions as control rod blocks, low CRD charging water header pressure trip bypass, 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/hot standby) 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.

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 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 3, 4, and 5 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 - Shutdown," LCO 3.10.4, "Control Rod Withdrawal - Cold Shutdown," and LCO 3.10.8, "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.

BASES

In MODE 6, with the reactor mode switch in the refuel position, only one control rod can be withdrawn under the refuel position one-rod-out interlock (LCO 3.9.2, "Refuel Position One-Rod/Rod-Pair-Out 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

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. Section 7.2.1.5.

2. Section 15.3.7.

B 3.10 SPECIAL OPERATIONS

B 3.10.3 Control Rod Withdrawal - Shutdown

BASES

BACKGROUND

The purpose of this MODE 3 and 4 Special Operations LCO is to permit the withdrawal of a single control rod for testing while in safe shutdown by imposing certain restrictions. In MODE 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 MODE 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 CRD hydraulic control unit) may be withdrawn by utilizing the Rod Test Switch, 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 MODE 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 MODE 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.

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 shutdown margin is maintained with any control rod pair fully withdrawn. When the rod test switch is used, the selected rod pair is substituted for a

BASES

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 the 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.

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.

BASES

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 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) Instrumentation," 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.

ACTIONS

A Note has been provided to modify the ACTIONS related to a single control rod or control rod pair withdrawal while in MODE 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.

A.1

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.

BASES

A.2.1 and A.2.2

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.

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. Section 15.3.

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 Rod Test Switch. 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 shutdown margin is maintained with any control rod pair fully withdrawn. When the rod test switch 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 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 3.9.1, 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 3.9.1, 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 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 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 is the highest worth control rod pair 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 pair may not be the highest worth control rod pair).
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 3.9.1, 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.

BASES

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 3.9.1, 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. 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. Section 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

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.

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 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

BASES

Completion Times for Required Action A.1, Required Action A.2.1, and Required Action A.2.2 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. Section 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 start-up 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 References 1 and 2. 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 References 1 and 2 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.

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

BASES

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 start-up range as defined in SR 3.3.2.1.6 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 the LPSP 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, “AVERAGE PLANAR LINEAR HEAT GENERATION RATE (APLHGR),” LCO 3.2.2, “MINIMUM CRITICAL POWER RATIO (MCPR),” LCO 3.2.3, “LINEAR HEAT GENERATION RATE (LHGR),” and LCO 3.3.2.1. With THERMAL POWER less than or equal to the LPSP of the RWM, 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. 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 - Safe 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 References 1 and 2 are satisfied. During these Special Operations and while in MODE 5, 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,” and LCO 3.9.5, “Control Rod

BASES

	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 3.3.2.1.6, which requires verification of the bypassing of control rods in RCIS and subsequent movement of these control rods.
REFERENCES	1. NEDE-24011-P-A-US, "General Electric Standard Application for Reactor Fuel," Supplement for United States (as amended). 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 start-up following refueling. Performing the SDM test prior to start-up 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 start-up or hot standby 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 start-up/hot standby position while in MODE 6, is provided by the Startup Range Neutron Monitor (SRNM) neutron flux scram (LCO 3.3.1.1, "Reactor Protection System (RPS) Instrumentation") and control rod block instrumentation (LCO 3.3.2.1, "Control Rod Block Instrumentation"). The limiting reactivity excursion during start-up 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 References 1 and 2 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 to the requirements of this LCO, will maintain normal test operations as well as postulated accidents within the bounds of the appropriate safety analyses (Refs. 1 and 2). In addition to the added requirements for the RWM, APRM, and control rod coupling, the notch out mode is specified for out-of-sequence withdrawals. Requiring the notch out 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 3.3.1.4, Functions 2.a and 2.d) 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 GWSR specified in LCO 3.1.6, “Rod Pattern Control” (i.e., out-of-sequence control rod withdrawals) must be made in the notched withdrawal 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 head may be removed during these tests, no other CORE ALTERATIONS may be in progress. In addition, the MODE 2 requirements for the reactor building are required to mitigate the

BASES

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 start-up or hot standby 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

With one or more control rods discovered uncoupled during this Special Operation, a controlled insertion of each uncoupled control rod is required; either to attempt recoupling, or to preclude an RWE. This controlled insertion is preferred since, if the control rod fails to follow the drive as it is withdrawn (i.e., is "stuck" in an inserted position), placing the reactor mode switch in the shutdown position per Required Action B.1 could cause substantial secondary damage. If recoupling is not accomplished, 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 3.3.2.1.6, if required, to allow insertion of inoperable control rod and continued operation. SR 3.3.2.1.6 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.

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

BASES

governed by subsequent entry into the Condition and application of the Required Actions.

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.

B.1

With the requirements of this LCO not met, the affected control rod shall be declared inoperable. 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, 3.10.8.2, and SR 3.10.8.3

LCO 3.3.1.4, Functions 2.a and 2.d, LCO 3.3.6.1, Functions 13 and 14, and LCO 3.6.3 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

SR 3.10.8.5

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. NEDE-24011-P-A-US, “General Electric Standard Application for Reactor Fuel,” Supplement for United States (as amended).

2. Section 15.3.