B 3.3 INSTRUMENTATION

B 3.3.1 Reactor Trip Instrumentation

BASES

BACKGROUND

The primary I&C systems used for control and monitoring in the plant are collectively referred to as the Distributed Control System (DCS). The DCS performs the majority of signal input processing, automation, operator interface, annunciation of abnormal process conditions, and actuator output functions in the plant. FSAR Section 7.1 (Ref. 1) describes the DCS and its constituent subsystems. The Protection System (PS) initiates a reactor trip (RT) to protect against violating the core specified acceptable fuel design limits and breaching the reactor coolant pressure boundary during anticipated operational occurrences (AOO). The PS also initiates (and the Safety Automation System (SAS) controls) the engineered safety features (ESF) actuations that are used to mitigate accidents. The ESF actuates necessary safety systems, based upon the values of selected plant parameters, to protect against violating core design limits, maintain the Reactor Coolant System (RCS) pressure boundary, and mitigate the consequences of accidents that could result in potential exposures comparable to the guidelines set forth in 10 CFR 100 during anticipated operational occurrences (AOOs) and ensures acceptable consequences during accidents.

The four redundant divisions of the DCS are physically separated in their respective safeguard buildings. The four divisionally separated rooms containing the DCS equipment are in different fire zones. Therefore, in general, the consequences of internal hazards (e.g., fire), would impact only one DCS division.

In general, the DCS architecture is four-fold redundant for both RT and ESF functions. A single failure during corrective or periodic maintenance, or a single failure and the effects of an internal hazard does not prevent performance of the safety functions. For the RT functions, each DCS division actuates one division of the RT devices based on redundant processing performed in four PS divisions. For ESF functions, the redundancy of the safety function as a whole is defined by the redundancy of the ESF system mechanical trains.

In general, this results in one DCS division actuating one mechanical train of an ESF system based on redundant processing performed in four PS divisions. The DCS not only supports the redundancy of the mechanical trains, but also enhances this redundancy through techniques such as redundant actuation voting.

BASES

BACKGROUND (continued)

In general, three of the four DCS divisions are necessary to meet the redundancy and testability of GDC 21 in 10 CFR 50, Appendix A (Ref. 2). The fourth division provides additional flexibility by allowing one division to be removed from service for maintenance or testing while still maintaining a minimum two out of three logic.

Each of the DCS sensors, function processors, or trip actuation devices can be placed in lockout, which renders the component inoperable. The signals within the PS carry a value and a status. The signal status can be propagated through the software function blocks; therefore, if an input signal to a function block has a faulty status, the output of the function block also has a faulty status. When a signal with a faulty status reaches the voting function block, the signal is disregarded through modification of the voting logic. Individual function processors can be put into a testing and diagnostic mode via the service unit. The function processor that is being tested then behaves like a processor with a “detected fault” for the system. The signal outputs are disabled and those sent via the communication modules are marked with the status “Test” or “Error” and therefore masked by selection blocks with active status processing. In this case the receiving function processor behaves as if the transmitting function processor has failed.

The protection and monitoring systems have been designed to ensure safe operation of the reactor. This is achieved by specifying limiting safety system settings (LSSS) in terms of parameters monitored by the DCS, as well as Limiting Conditions for Operation (LCO) on other reactor system parameters and equipment performance. The subset of LSSS that directly protect against violating the reactor core and RCS pressure boundary safety limits during AOOs are referred to as Safety Limit LSSS (SL-LSSS).

Technical Specifications are required by 10 CFR 50.36 to contain LSSS defined by the regulation as "...settings for automatic protective devices...so chosen that automatic protective actions will correct the abnormal situation before a Safety Limit (SL) is exceeded." The Analytical Limit is the limit of the process variable at which a safety action is initiated, as established by the safety analysis, to ensure that an SL is not exceeded. Any automatic protection action that occurs on reaching the Analytical 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 Analytical Limit to account for instrument loop uncertainties related to the setting at which the automatic protective action would actually occur.

BASES

BACKGROUND (continued)

The Nominal Trip Setpoint (NTSP) is a predetermined setting for a protective device chosen to ensure automatic actuation prior to the process variable reaching the Analytical Limit and thus ensuring that the SL would not be exceeded. As such, the NTSP 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 (Ref. 3)). In this manner, the NTSP ensures that SLs are not exceeded. As such, the NTSP meets the definition of an SL-LSSS (Ref. 4). The Analytical Limits are determined as part of the safety analysis (Ref. 5). NTSPs and Analytical Limits are addressed in the Technical Specifications in accordance with Specification 5.5.19, “Setpoint Control Program.”

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)." However, the use of sensor calibration settings to define OPERABILITY in Technical Specifications would be an overly restrictive requirement if applied as the OPERABILITY limits for the "as-found" values of sensing device calibration settings during performance of Surveillances. 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, a sensing device with an as-found sensor calibration setting value that has been found to be different from the specified calibration setting due to some drift of the sensor 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 NTSP and thus the automatic protective action would still have ensured that the SL would not be exceeded with the "as-found" value of the sensing device. Therefore, the sensing device would still be OPERABLE since it would have performed its safety function and the only corrective action required would be to calibrate the sensor to account for further drift during the next surveillance interval.

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. The Allowable Value is the least conservative value of the as-found sensor calibration setting that a sensor can have when tested such that the sensor is OPERABLE if the as-found sensor calibration setting value is conservative with respect to the Allowable Value during a

BASES

BACKGROUND (continued)

CALIBRATION. As such, the Allowable Value differs from the sensor calibration setting by an amount greater than or equal to the expected instrument loop uncertainties, such as drift, during the surveillance interval. In this manner, the CALIBRATION of the device will ensure that an SL is not exceeded at any given point in time as long as the device has not drifted beyond that expected during the surveillance interval. Note that, although the sensor is OPERABLE under these circumstances, the as-left sensor calibration setting values must be set or confirmed to be within the as-left tolerance around the specified calibration settings at the completion of the surveillance, and confirmed to be operating within the statistical allowances of the uncertainty terms assigned (as-found). If the actual sensor calibration setting value is found to be non-conservative with respect to the Allowable Value, the sensor 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.

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

– The departure from nucleate boiling ratio (DNBR) shall be maintained above the SL value to prevent departure from nucleate boiling (DNB),
– Fuel centerline melting shall not occur; and
– The RCS pressure SL of 2803 psia shall not be exceeded.

Maintaining the parameters within the above values ensures that the offsite dose will be within the 10 CFR 100 (Ref. 6) criteria during AOOs.

Accidents are events that are analyzed even though they are not expected to occur during the plant life. The acceptable limit during accidents is that the offsite dose shall be maintained within an acceptable fraction of 10 CFR 100 limits. Different accident categories are allowed a different fraction of these limits, based on probability of occurrence. Meeting the acceptable dose limit for an accident category is considered having acceptable consequences for that event.

The PS is an integrated reactor protection system and engineered safety features actuation system. Individual sensors, function processors, (i.e., Acquisition and Processing Units (APU) or Actuation Logic Units (ALU)) that provide the actuation signal voting function, can be associated with multiple RTs, ESF functions, and permissives.

BASES

BACKGROUND (continued)

The PS is segmented into three interconnected modules and associated LCOs for the Trip/ESF/Permissive Functions. These modules are:

– Input & Acquisition Logic Division: The portion of the logic that reads in the plant parameter (e.g. pressurizer pressure) and performs further conditioning (e.g. filters), calculations, comparison of values to setpoints, and sending to the voting logic. The hardware includes the sensor and associated conditioning equipment (e.g. Incore Instrumentation System and the Signal Conditioning and Distribution System (SCDS)), the APU, and cabling to the ALUs.
– Actuation Logic Division: The portion of the logic that receives the partial trigger value from the Input & Acquisition Logic and provides further calculation, voting, and logic before sending an actuation signal. The hardware includes the ALU, hardwired logic downstream of the ALU, and cabling to the priority and actuator control system (PACS) or RT devices.
– Manual Division: The portion of the logic that provides a manual input to the Actuation Logic Division (system-level) or PACS (component-level). The hardware includes the manual device (Safety Information and Control System (SICS) pushbutton) and cabling to the Actuation Logic Division or PACS or RT devices.

The instrument setpoint methodologies used for the U.S. EPR were submitted to NRC in References 4 and 7. The majority of RTs or protection functions are based on single division inputs; therefore, the uncertainties identified in Section 3.1 of Reference 4 are applicable for the trip. Reference 7 addresses the protection system trips or protection functions that are based on multiple inputs. The uncertainty calculations for the Self-Powered Neutron Detectors (SPND), incore instrumentation, high linear power density, high core power level, low saturation margin, anti-dilution, and DNBR use the statistical methodology described in Reference 7. As described therein, the NTSP is the LSSS since all known errors are appropriately combined in the total loop uncertainty calculation.

NTSPs that are in accordance with the Allowable Value will ensure that SLs of Chapter 2.0, "Safety Limits (SLs)," are not violated during AOOs, and the consequences of postulated accidents will be acceptable, providing the plant is operated from within the LCOs at the onset of the AOO or postulated accident and the equipment functions as designed.

BASES

BACKGROUND (continued)

Note that the Allowable Value is the least conservative value of the as-found sensor calibration setting value that a sensor can have during a periodic CALIBRATION, such that the sensor is OPERABLE if the as-found sensor calibration setting value is conservative with respect to the Allowable Value.

Functional testing of the entire DCS, from sensor input through the opening of individual sets of Reactor Trip Breakers (RTB) or Reactor Trip Contactors (RTC), is performed each refueling cycle. Process transmitter CALIBRATION is also normally performed on a refueling basis.

RT setpoints that directly protect against violating the reactor core or RCS pressure boundary Safety Limits during AOOs are SL-LSSS. Permissive setpoints allow bypass of trips when they are not required by the Safety Analysis. These permissives ensure that the starting conditions are consistent with the safety analysis, before preventative or mitigating actions occur. The permissives are only one of multiple conservative starting assumptions for the accident analysis. Therefore, permissive setpoints are not considered to be SL-LSSS. Each specified NTSP is more conservative than the Analytical Limit assumed in the safety analysis in order to account for instrument uncertainties appropriate to the trip function. The methodologies for considering uncertainties are defined in References 4 and 7.

Protection System

The PS is a distributed, redundant computer system. It consists of four independent redundant data-processing automatic paths (divisions), each with layers of operation and running asynchronous with respect to each other. In addition to the computers associated with the automatic paths, there are two message and service interface computers to interface with each division.

Each SCDS division acquires analog and binary input signals from sensors in the plant (such as for temperature, pressure, and level measurements). Each SCDS division distributes its acquired and preprocessed input signals to the PS data processing computers (i.e., APU).

The APUs perform signal processing for plant protective functions such as signal online validation, limit value monitoring and calculations. Each PS division contains five APUs, two assigned to one subsystem and three assigned to the other subsystem. The APUs then send their outputs to two independent voter function processors (i.e., ALU). Each PS division

BASES

BACKGROUND (continued)

contains four ALUs, two assigned to each subsystem. Two ALUs of the same subsystem within a division are redundant and perform the same processing using the same inputs. The outputs of two redundant ALUs are combined in a hardwired “functional AND” logic for RT functions and in a hardwired “functional OR” logic for ESF functions. This avoids both unavailability of ESF functions and spurious RTs.

In the ALUs, the outputs of the APUs of redundant divisions are processed together. An ALU controls a set of actuators. Each ALU receives the actuation signal from each of the redundant APUs. The ALU's task is to compare this redundant information and compute a validated (voted) actuating signal, which is used for actuating the end devices.

When an APU is placed in lockout, network outputs are marked as invalid and are disregarded in downstream processing. For example, a two out of four voting function that receives one faulty input, votes two out of three on the remaining non-faulty inputs. Hardwired outputs (i.e., ALU outputs) are forced to a no output state, resulting in a RT signal and no ESF actuation. No manual actions, beyond placing the function processor in lockout, are required for the downstream processing to properly accommodate the function processor in a lockout condition.

Reactor Trip Logic

Critical plant parameters such as temperatures, pressures, and levels are sensed, acquired, and converted to electrical signals by the SCDS. These signals are sent to various RT functions in the PS where they are processed. When prohibited operating conditions exist, a reactor trip signal is generated from the reactor trip functions. Besides being generated automatically from the PS, a reactor trip signal can also be generated from the following systems:

– Automatic reactor trip from the Diverse Actuation Instrumentation in the unlikely event of a software common cause failure of the PS;
– Manual reactor trip from the Main Control Room (MCR); and
– Manual reactor trip from the RSS. Note that the RSS manual reactor trip is not part of the required circuits for LCO 3.3.1.

The reactor trip functions will utilize voting logic in order to screen out potential upstream failures of sensors or function processors.

The architecture of the PS, as well as logic implemented in the PS, will guard against spurious reactor trip orders while ensuring that those orders will be available when needed.

BASES

BACKGROUND (continued)

Single failures upstream of the ALU layer that could result in an invalid signal being used in the reactor trip function are accommodated by modifying the vote in the ALU layer. For the reactor trip functions, the vote is always modified toward reactor trip.

The reactor trip outputs of the two OPERABLE redundant ALUs in a subsystem are combined in a hardwired “functional AND” configuration. This requires both ALUs to output the reactor trip signal for the associated Trip Actuation Device to be actuated. The outputs of the “functional AND’ from both subsystems within a division are combined in a “functional OR” logic. The “functional AND” provides protection against spurious reactor trips while maintaining the ability to actuate a trip if an ALU has failed. However, if only one ALU in a subsystem is OPERABLE, the subsystem is still OPERABLE, and the single voting ALU will initiate a reactor trip.

There are four dedicated reactor trip buttons in the MCR, one for each division. Any two of these buttons together will actuate a reactor trip.

Reactor Trip Actuation Devices

The reactor trip actuation is performed by interrupting electrical power to the Control Rod Drive Mechanism (CRDM). Electrical power to the CRDM is delivered by the Non-Class 1E Uninterruptible Power Supply System. The power supply of the CRDM can be switched off via the following features:

– Four RTBs distributed in two electrical divisions. Two RTBs are located in Division 2, two others in Division 3. The RTBs can be opened by two coils: one with a de-energized logic using an under voltage coil and the other with an energized logic using a shunt trip coil. The under voltage coil of the RTBs is actuated by the automatic reactor trip signals of the PS and the manual reactor trip from the SICS panel. The shunt coil of the RTBs is actuated by the automatic reactor trip signal from the Diverse Actuation Instrumentation and the manual reactor trip signal from the RSS.
– The reactor trip signal generated automatically by the PS and the manual reactor trip signal generated from the SICS panel actuates the RTCs. There are 23 sets of four RTCs, each set capable of removing power to four CRDM power supplies. Eleven sets of contactors are located in Division 1 and twelve sets are located in Division 4. Each division of the PS is assigned to one contactor in each of the 23 sets. Each set of four contactors is arranged to require at least two reactor trip orders to drop the rods assigned to the contactor set.

BASES

BACKGROUND (continued)

Once open, the RTBs require manual closure and they cannot be manually closed until the reactor trip signal is cleared by the PS.

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

The DCS is designed to ensure that the following operational criteria are met:

– The associated actuation will occur when the parameter monitored by each division reaches its setpoint and the specific coincidence logic is satisfied; and
– In general, separation and redundancy are maintained to permit a division to be out of service for testing or maintenance while still maintaining redundancy within the DCS instrumentation network.

Each of the analyzed transients and accidents can be detected by one or more PS functions. Each of the reactor trips included in the Technical Specifications are credited as part of the primary success path in the accident analysis. Therefore, the Reactor Trip Instrumentation satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii). Non-credited automatic functions are not included in the Technical Specifications. Refer to FSAR Sections 7.2 for a description of the reactor trip functions. Credited functions are included in FSAR Table 15.0-7.

In general, the DCS Input & Acquisition Logic Division, Actuation Logic Division, and Manual Division that support reactor trips are required to be OPERABLE in MODES 1, 2 and/or 3 because the reactor is or can be made critical in these MODES. The automatic reactor trip functions are designed to take the reactor subcritical, which maintains the SLs during AOOs and assists the ESF in providing acceptable consequences during accidents.

The specific safety analysis and OPERABILITY requirements applicable to each DCS protective function are identified below. Permissives are addressed in LCO 3.3.3, “Permissive Instrumentation.”

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

The Reactor Trip Instrumentation Functions are:

1-5. Departure from Nucleate Boiling Ration (DNBR) - Low

These trips protect the fuel against the risk of departure from nucleate boiling during AOOs that lead to a decrease of the DNBR value. There are five Low DNBR trips:

1. DNBR - Low,
2. DNBR with High Quality – Low,
3. DNBR with Imbalance or Rod Drop (1/4) – Low,
4. DNBR with High Quality and (Imbalance or Rod Drop) (1/4) – Low, and
5. DNBR with Rod Drop (2/4) – Low.

Together, these five trips protect against the following postulated accidents or AOOs:

– Increase in heat removal by the secondary system,
– Decrease in heat removal by the secondary system,
– Reactivity and power distribution anomalies, and
– Decrease in reactor coolant inventory.

Four divisions of the DNBR – Low (1) and DNBR with High Quality - Low (2) trip functions are required to be OPERABLE in MODE 1 with P2 permissive validated.

These trips utilize the following sensors:

– SPNDs (addressed in LCO 3.3.14, “Self-Powered Neutron Detectors (SPND),”
– RCP Speed sensors,
– Pressurizer Pressure (Narrow Range) sensors,
– Cold Leg Temperature (Narrow Range) sensors, and
– RCS Loop Flow sensors.

Four divisions of the DNBR with Imbalance or Rod Drop (1/4) – Low (3), DNBR with High Quality and (Imbalance or Rod Drop) (1/4) – Low (4), and DNBR with Rod Drop (2/4) – Low (5) trip functions are required to be OPERABLE in MODE 1 with P2 permissive validated.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

These trips utilize the following sensors:

– SPNDs (addressed in LCO 3.3.14, “Self-Powered Neutron Detectors (SPND),”
– Rod Cluster Control Assembly (RCCA) Analog Position Indication sensors,
– RCP Speed sensors,
– Pressurizer Pressure (Narrow Range) sensors,
– Cold Leg Temperature (Narrow Range) sensors, and
– RCS Loop Flow sensors.

The NTSPs are low enough to provide an operating envelope that prevents an unnecessary low DNBR reactor trip. The NTSPs are high enough for the system to maintain a margin to unacceptable fuel cladding damage for AOOs that leads to an uncontrolled decrease of the DNBR value.

Validation of the P2 permissive automatically enables the five Low DNBR trip signals when the reactor power level, as measured by the Power Range Detectors, is greater than approximately 10% RTP. When power is less than or equal to this threshold, the trips are automatically disabled by inhibition of the P2 permissive.

6. Linear Power Density - High

This trip protects the fuel against the risk of melting at the center of the fuel pellet, during AOOs that lead to an uncontrolled increase of the linear power density. This trip protects against the following postulated accidents or AOOs:

– Increase in heat removal by the secondary system, and
– Reactivity and power distribution anomalies.

Four divisions of the Linear Power Density - High trip function are required to be OPERABLE in MODE 1 with P2 permissive validated.

This trip utilizes the SPNDs. SPNDs are addressed in LCO 3.3.14, “Self-Powered Neutron Detectors (SPND).”

The NTSP is high enough to provide an operating envelope that prevents unnecessary Linear Power Density - High trips. The NTSP is low enough for the system to maintain a margin to unacceptable fuel centerline melt for any AOOs that lead to an uncontrolled increase of the linear power density.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

Validation of the P2 permissive automatically enables the reactor trip signal when the reactor power level, as measured by the Power Range Detectors, is greater than approximately 10% RTP. When power is less than or equal to this threshold, the trip is automatically disabled by inhibition of the P2 permissive.

7. Neutron Flux Rate of Change - High

This trip limits the consequences of an excessive reactivity increase from a range in reactor power levels, including RTP. This trip protects against reactivity and power distribution anomalies.

Four divisions of the Neutron Flux Rate of Change - High trip function are required to be OPERABLE in:

– MODES 1, 2, and
– MODE 3 with the RCSL System capable of withdrawing an RCCA or one or more RCCAs not fully inserted.

This trip utilizes the following Power Range Detectors.

The NTSP is high enough to provide an operating envelope that prevents unnecessary High Neutron Flux Rate of Change (Power Range) reactor trips. The NTSP is low enough for the system to maintain a margin to unacceptable fuel cladding damage due to an excessive reactivity increase.

There are no permissives associated with this trip.

8. Core Power Level - High

This trip limits the consequences of an excessive reactivity increase from a range in reactor power levels, including RTP. This trip protects against the following postulated accidents or AOOs:

– Increase in heat removal by the secondary system, and
– Reactivity and power distribution anomalies.

Four divisions of the Core Power Level - High trip function are required to be OPERABLE in:

– MODE 1, and
– MODE 2 with P5 permissive validated.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

This trip utilizes the following sensors:

– Cold Leg Temperature (Wide Range) sensors,
– Hot Leg Pressure (Wide Range) sensors,
– Hot Leg Temperature (Narrow Range) sensors, and
– RCS Loop Flow sensors.

The NTSP is high enough to provide an operating envelope that prevents an unnecessary High Core Power Level reactor trip. The NTSP is low enough for the system to maintain a margin to unacceptable fuel cladding damage due to an excessive reactivity increase from a range in reactor power levels, including RTP.

Validation of the P5 permissive automatically enables the High Core Power Level trip when the reactor power level is greater than approximately 10^{-5}% RTP. Inhibition of the P5 permissive automatically disables the High Core Power Level trip when less than or equal to this threshold.

9. Saturation Margin - Low

This trip provides a reactor trip before saturation occurs in a hot leg. The Core Power Level - High trip relies on RCS loop temperature measurements as part of the calculation of thermal and hydraulic conditions. The Core Power Level - High calculation would not be valid if saturation were to occur in a hot leg. Therefore, the Saturation Margin - Low reactor trip is introduced because, in case of saturation occurring in a hot leg, the thermal core power level calculation becomes invalid.

Four divisions of the Saturation Margin – Low trip function are required to be OPERABLE in:

– MODE 1, and
– MODE 2 with P5 permissive validated.

This trip utilizes the following sensors:

– Cold Leg Temperature (Wide Range) sensors,
– Hot Leg Pressure (Wide Range) sensors,
– Hot Leg Temperature (Narrow Range) sensors, and
– RCS Loop Flow sensors.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

The NTSP is low enough to provide an operating envelope that prevents an unnecessary Saturation Margin - Low reactor trip. The NTSP is high enough for the system to maintain a margin to unacceptable fuel cladding damage during AOOs.

Validation of the P5 permissive automatically enables the Saturation Margin - Low trip when the reactor power level is greater than approximately 10^{-5} % RTP. Inhibition of the P5 permissive automatically disables the Saturation Margin - Low trip when less than or equal to this threshold.

10. RCS Flow Rate – Low in Two Loops

This trip initiates a reactor trip and is inhibited below a certain level of nuclear power under which the protection is not necessary because DNB is no longer a risk in this condition. This trip protects against the following postulated accidents or AOOs:

– Decrease in heat removal by the secondary system, and
– Decrease in RCS flow rate.

Four divisions of the RCS Flow Rate – Low in Two Loops trip function are required to be OPERABLE in MODE 1 with P2 permissive validated.

This trip utilizes the RCS Loop Flow sensors.

The NTSP is low enough to provide an operating envelope that prevents unnecessary RCS Flow Rate – Low in Two Loops reactor trips. The NTSP is high enough for the system to maintain a margin to ensure DNBR limits are met for AOOs.

Validation of the P2 permissive automatically enables the RCS Flow Rate - Low in Two Loops trip when the reactor power level is greater than approximately 10% RTP. Inhibition of the P2 permissive automatically disables the RCS Flow Rate – Low in Two Loops trip when less than or equal to this threshold.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

11. RCS Flow Rate – Low-Low in One Loop

This trip initiates a reactor trip and is inhibited below a certain level of nuclear power under which the protection is not necessary because DNB is no longer a risk in this condition. This trip protects against the following postulated accidents or AOOs:

– Decrease in heat removal by the secondary system, and
– Decrease in RCS flow rate.

Four divisions of the RCS Flow Rate – Low-Low in One Loop trip function are required to be OPERABLE in MODE 1 with P3 permissive validated.

This trip utilizes the RCS Loop Flow sensors.

The NTSP is low enough to provide an operating envelope that prevents unnecessary RCS Flow Rate – Low-Low in One Loop reactor trips. The NTSP is high enough for the system to maintain a margin to ensure DNBR limits are met for AOOs and bounded for postulated accidents.

Validation of the P3 permissive automatically enables the RCS Flow Rate – Low-Low in One Loop trip when the reactor power level is greater than approximately 70% RTP. Inhibition of the P3 permissive automatically disables the RCS Flow Rate – Low-Low in One Loop trip when less than or equal to this threshold.

12. RCP Speed – Low in Two Loops

Due to electrical transients that may affect the RCPs, a specific protection function is required. This function initiates a reactor trip and is inhibited below a low level of reactor power under which the protection is not necessary because DNB is no longer a risk. This trip protects against the following postulated accidents or AOOs:

– Decrease in heat removal by the secondary system, and
– Decrease in RCS flow rate.

Four divisions of the RCP Speed – Low in Two Loops trip function are required to be OPERABLE in MODE 1 with P2 permissive validated.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

This trip utilizes the RCP Speed sensors.

The NTSP is low enough to provide an operating envelope that prevents unnecessary RCP Speed – Low in Two Loops reactor trips. The NTSP is high enough for the system to maintain a margin to ensure DNBR limits are met for AOOs.

Validation of the P2 permissive automatically enables the RCP Speed - Low in Two Loops trip when the reactor power level is greater than approximately 10% RTP. When the reactor power level is less than or equal to this threshold, the trip is automatically disabled by inhibition of the P2 permissive.

13. Neutron Flux - High (Intermediate Range)

This trip limits the consequences of an excessive reactivity increase when the reactor is started up from a sub-critical or low power start-up condition. This trip protects against reactivity and power distribution anomalies.

Four divisions of the Neutron Flux - High (Intermediate Range) trip function are required to be OPERABLE in:

– MODE 1 with P6 permissive inhibited,
– MODE 2, and
– MODE 3 with the RCSL System capable of withdrawing an RCCA or one or more RCCAs not fully inserted.

This trip utilizes the Intermediate Range Detectors.

The NTSP is high enough to provide an operating envelope that prevents an unnecessary Neutron Flux - High (Intermediate Range) reactor trip. The NTSP is low enough for the system to maintain a margin to unacceptable fuel cladding damage for AOOs that leads to an uncontrolled increase of the linear power density.

Inhibition of the P6 permissive automatically enables the Neutron Flux - High (Intermediate Range) reactor trip when the reactor power level is less than or equal to approximately 10% RTP. When the reactor power level is above this threshold, the trip is disabled by manual validation of the P6 permissive.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

14. Doubling Time – Low

This trip limits the consequences of an excessive reactivity increase when the reactor is started up from a sub-critical or low power start-up condition. This trip protects against reactivity and power distribution anomalies.

Four divisions of the Doubling Time – Low trip function are required to be OPERABLE in:

– MODE 1 with P6 permissive inhibited,
– MODE 2, and
– MODE 3 with the RCSL System capable of withdrawing an RCCA or one or more RCCAs not fully inserted.

This trip utilizes the Intermediate Range Detectors.

The NTSP is high enough to provide an operating envelope that prevents an unnecessary Doubling Time – Low reactor trip. The NTSP is low enough for the system to maintain a margin to unacceptable fuel cladding damage for any postulated event that leads to an uncontrolled increase of the linear power density.

Inhibition of the P6 permissive automatically enables the Doubling Time – Low reactor trip when the reactor power level is less than or equal to approximately 10% RTP. When the reactor power level is above this threshold, the trip is disabled by manual validation of the P6 permissive.

15. Pressurizer Pressure - Low

A RCS depressurization may lead to a risk of excessive boiling, thus a reactor trip is required to ensure fuel rod integrity and to adapt reactor power to the capacity of the safety systems. This trip protects against a decrease in reactor coolant inventory.

Four divisions of the Pressurizer Pressure - Low trip function are required to be OPERABLE in MODE 1 with P2 permissive validated.

This trip utilizes the Pressurizer Pressure (Narrow Range) sensors.

The NTSP is sufficiently below the full load operating value for RCS pressure so as not to interfere with normal plant operation, but still high enough to provide the required protection in the event of an RCS depressurization.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

Validation of the P2 permissive automatically enables the Pressurizer Pressure - Low trip when the reactor power level is greater than approximately 10% RTP. When the reactor power level is less than or equal to this threshold, the trip is automatically disabled by inhibition of the P2 permissive.

16. Pressurizer Pressure - High

In case of an RCS overpressure, a reactor trip is required in order to:

– Adapt the reactor power to the capacity of the safety systems,
– Ensure RCS integrity, and
– Avoid opening of the Pressurizer safety valves in certain primary side overpressure transients.

This trip protects against a decrease in heat removal by the secondary system.

Four divisions of the Pressurizer Pressure - High trip function are required to be OPERABLE in MODES 1 and 2.

This trip utilizes the Pressurizer Pressure (Narrow Range) sensors.

The NTSP is sufficiently below the nominal lift setting of the Pressurizer Safety Relief Valves (PSRV), and its operation avoids the undesirable operation of these valves during normal plant operation. In the event of a complete loss of electrical load from 100% power, this setpoint ensures the reactor trip will take place, thereby limiting further heat input to the RCS and consequent pressure rise. The PSRVs may lift to prevent overpressurization of the RCS.

There are no permissives associated with this trip.

17. Pressurizer Level - High

In case of increasing Pressurizer level, a reactor trip is required in order to avoid Pressurizer overfilling. This trip protects against increases in reactor coolant inventory.

Four divisions of the Pressurizer Level - High trip function are required to be OPERABLE in:

– MODE 1, and
– MODE 2 with P12 permissive inhibited.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

This trip utilizes the Pressurizer Level (Narrow Range) sensors.

The NTSP is sufficiently below the point where the associated transient would reach the nominal lift setting of the PSRVs, and its operation avoids the undesirable operation of these valves during normal plant operation. In the event of a CVCS malfunction, this setpoint ensures a timely reactor trip will take place in order to avoid filling the pressurizer. The PSRVs may lift to prevent overpressurization of the RCS.

Inhibition of the P12 permissive automatically enables the Pressurizer Level - High trip when the pressurizer pressure is greater than or equal to approximately 2005 psia. When below this threshold, the trip is disabled by manual validation of the P12 permissive.

18. Hot Leg Pressure - Low

A RCS depressurization may lead to a risk of excessive boiling, thus a reactor trip is required to ensure fuel rod integrity and to adapt reactor power to the capacity of the safety systems. This trip protects against a decrease in reactor coolant inventory.

Four divisions of the Hot Leg Pressure - Low trip function are required to be OPERABLE in:

– MODES 1, 2, and
– MODE 3 with P12 permissive inhibited and with the RCSL System capable of withdrawing an RCCA or one or more RCCAs are not fully inserted.

This trip utilizes the Hot Leg Pressure (Wide Range) sensors.

The NTSP is sufficiently below the full load operating value so as not to interfere with normal plant operation, but still high enough to provide the required protection in the event of abnormal conditions.

Inhibition of the P12 permissive automatically enables the Hot Leg Pressure - Low trip when the pressure is greater than or equal to approximately 2005 psia. When below this threshold, the trip is disabled by manual validation of the P12 permissive.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

19. SG Pressure Drop – Low

In case of steam or feedwater system piping failure, the affected Steam Generator (SG) depressurizes leading to an RCS cooldown or heatup. A reactor trip is required in order to ensure the fuel rod integrity and to adapt the reactor power to the capacity of the safety systems. This trip protects against the following postulated accidents or AOOs:

– Increase in heat removal by the secondary system, and
– Decrease in heat removal by the secondary system.

Four divisions of the SG Pressure Drop – Low trip Function are required to be OPERABLE in:

– MODES 1, 2, and
– MODE 3 with the RCSL System capable of withdrawing an RCCA or one or more RCCAs not fully inserted.

This trip utilizes the SG Pressure sensors.

The condition to be detected is an SG pressure drop greater than a specified value. This is accomplished by using a variable pressure setpoint tracking the steam line pressure with a constant offset. The setpoint has a limitation on its maximum pressure and its maximum rate of decrease. If the steam line pressure increases, the setpoint will increase until the limitation on maximum pressure is reached. If the steam line pressure decreases, the setpoint will follow the decrease as long as the rate is less than or equal to the limitation on maximum rate of decrease. If the steam line pressure decreases more rapidly than the limitation on the maximum rate of decrease, the margin between the actual pressure and the setpoint will decrease until the steam line pressure equals the setpoint and protective action occurs.

The NTSP is sufficiently below the full load operating value so as not to interfere with normal plant operation, but still high enough to provide the required protection in the event of a pipe break.

There are no permissives associated with this trip.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

20. SG Pressure - Low

In case of steam or feedwater system piping failure, the affected SG depressurizes leading to an RCS cooldown or heatup. For small breaks, the setpoint of the reactor trip on SG Pressure Drop may not be reached. Therefore, a reactor trip on SG Pressure - Low is introduced in order to ensure fuel rod integrity and to adapt the reactor power to the capacity of safety systems. This trip protects against the following postulated accidents or AOOs:

– Increase in heat removal by the secondary system, and
– Decrease in heat removal by the secondary system.

Four divisions of the SG Pressure - Low trip function are required to be OPERABLE in:

– MODES 1, 2, and
– MODE 3 with P12 permissive inhibited and with the RCSL System capable of withdrawing an RCCA or one or more RCCAs not fully inserted.

This trip utilizes the SG Pressure sensors.

The NTSP is sufficiently below the full load operating value so as not to interfere with normal plant operation, but still high enough to provide the required protection in the event of a pipe break.

Inhibition of the P12 permissive automatically enables the SG Pressure - Low trip when the pressure is greater than or equal to approximately 2005 psia. When below this threshold, the trip is disabled by manual validation of the P12 permissive.

21. SG Pressure - High

In case of a loss of the main heat sink, the reactor has to be tripped in order to:

– Ensure fuel rods integrity at power,
– Adapt the reactor power to the capacity if safety systems, and
– Ensure SG integrity.

This trip protects against a decrease in heat removal by the secondary system.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

Four divisions of the SG Pressure - High trip function are required to be OPERABLE in MODE 1.

This trip utilizes the SG Pressure sensors.

The NTSP is high enough to avoid spurious operation. In case of a loss of the main heat sink, the NTSP is low enough to trip the reactor in order to:

– Ensure fuel rod integrity at power,
– Adapt the reactor power to the capacity of safety systems, and
– Ensure SG integrity.

There are no permissives associated with this trip.

22. SG Level - Low

This trip protects the reactor from a loss of heat sink in case of SG steam/feedwater flow mismatch. This trip protects against a decrease in heat removal by the secondary system.

Four divisions of the SG Level – Low Level trip function are required to be OPERABLE in:

– MODE 1, and
– MODE 2 with P13 permissive inhibited.

This trip utilizes the SG Level (Narrow Range) sensors.

The NTSP is sufficiently below the full load operating value so as not to interfere with normal plant operation, but still high enough to provide the required protection in the event of a flow mismatch.

Inhibition of the P13 permissive automatically enables the SG Level - Low trip when the hot leg temperature is greater than or equal to approximately 200°F. When below this threshold, the trip is disabled by manual validation of the P13 permissive.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

23. SG Level - High

This trip protects the turbine against moisture carryover in case of a main feedwater (MFW) malfunction causing an increase in feedwater flow or in case of SG level increase. This reactor trip ensures core integrity during these transients since an increase in feedwater flow leads to an RCS overcooling event and hence a reactivity insertion. This trip protects against an increase in heat removal by the secondary system.

Four divisions of the SG Level - High trip function are required to be OPERABLE in:

– MODES 1, 2, and
– MODE 3 with P13 permissive inhibited and the RCSL System capable of withdrawing an RCCA or one or more RCCAs not fully inserted.

This trip utilizes the SG Level (Narrow Range) sensors.

The NTSP is sufficiently above the full load operating value so as not to interfere with normal plant operation, but still low enough to provide the required protection in the event of an abnormal condition.

Inhibition of the P13 permissive automatically enables the SG Level - High trip when the hot leg temperature is greater than or equal to approximately 200°F. When below this threshold, the trip is disabled by manual validation of the P13 permissive.

24. Containment Pressure - High

In case of a postulated high energy initiating event leading to water or steam discharge into the containment, a reactor trip is performed in order to ensure containment integrity and to adapt the reactor power to the capacity of the safety systems. This trip protects against the following postulated accidents or AOOs:

– Increase in heat removal by secondary system,
– Decrease in heat removal by the secondary system, and
– Decrease in reactor coolant inventory.

This trip is also necessary to actuate the Containment Isolation (Stage 1) - High Containment Pressure ESF function.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

Four divisions of the Containment Pressure - High trip function are required to be OPERABLE in:

– MODES 1, 2, and
– MODE 3 with the RCSL System capable of withdrawing an RCCA or one or more RCCAs not fully inserted.

This trip utilizes the following sensors:

– Containment Equipment Compartment Pressure sensors, and
– Containment Service Compartment Pressure (Narrow Range) sensors.

The NTSP is high enough to allow for small pressure increases in containment expected during normal operation (i.e., plant heatup) and is not indicative of an abnormal condition. It is low enough to initiate a reactor trip when an abnormal condition is indicated.

There are no permissives associated with this trip.

25. Safety Injection Actuation - Automatic

This function is provided to trip the reactor when the Safety Injection Signal (SIS) is automatically actuated by the PS. In each division of the PS, when a SIS Actuation signal is generated, a reactor trip order is also generated in the same division.

Four divisions of the reactor trip on Safety Injection Actuation - Automatic function are required to be OPERABLE in MODES 1 and 2.

The sensors required to generate the SIS Actuation signal are identified under each separate automatic ESF function:

– SIS Actuation - Low Pressurizer Pressure (ESF 1.a),
– SIS Actuation - Low Delta P_{sat} (ESF 1.b), and
– SIS Actuation – Low Hot Leg Loop Level (ESF 1.c).

There are no permissives associated with this trip.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

26. Emergency Feedwater System Actuation – Low-Low SG Level

This function is provided to trip the reactor when the EFWS is actuated by the PS due to low SG level. In each division of the PS, when an EFWS Actuation signal is generated due to low SG level (regardless of the EFWS train to be initiated), a reactor trip signal is also generated in the same division.

Four divisions of the reactor trip on Emergency Feedwater System Actuation – Low-Low SG Level Function are required to be OPERABLE in MODES 1 and 2.

The sensors required to generate the Emergency Feedwater System Actuation – Low-Low SG Level signal are identified under ESF 2.a: EFWS Actuation - Low-Low SG Level (Affected SG).

There are no permissives associated with this trip.

27. Manual Rector Trip - Manual

Manual actuation switches are available in the SICS in the Main Control Room. There is one manual Reactor Trip switch per division. Any two together will actuate a reactor trip.

The four manual Reactor Trip switches are required to be OPERABLE in:

– MODES 1, 2, and
– MODES 3 with the RCSL System capable of withdrawing an RCCA or one or more RCCAs not fully inserted.

A Manual Reactor Trip accomplishes the same results as any one of the automatic trip Functions. It is used by the reactor operator to shut down the reactor whenever any parameter is rapidly trending toward its Trip Setpoint.

There is no NTSP associated with this Function.

There are no permissives associated with this Function.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

28. Reactor Trip Breakers

There are two RTBs in Divisions 2 and 3 only.

Two RTBs per division (Divisions 2 and 3 only) are required to be OPERABLE in:

– MODES 1 and 2, and
– MODES 3 with the RCSL System capable of withdrawing an RCCA or one or more RCCAs not fully inserted.

These trip actuation devices support the reactor trip functions.

This Function does not utilize any sensors.

There is no NTSP associated with this Function.

There are no permissives associated with this Function.

29. Reactor Trip Contactors

There are four RTCs in each of twenty-three sets in Divisions 1 and 4 only.

Four RTCs in each of twenty-three sets per division (Divisions 1 and 4 only) are required to be OPERABLE in:

– MODES 1 and 2, and
– MODE 3 with the RCSL System capable of withdrawing an RCCA or one or more RCCAs not fully inserted.

These trip actuation devices support the reactor trip functions.

This Function does not utilize any sensors.

There is no NTSP associated with this Function.

There are no permissives associated with this Function.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

30. Actuation Logic

Four divisions of the Actuation Logic are required to be OPERABLE in:

– MODES 1 and 2, and
– MODE 3 with the RCSL System capable of withdrawing an RCCA or one or more RCCAs not fully inserted.

This Function does not utilize any sensors.

There is no NTSP associated with this Function.

There are no permissives associated with this Function

ACTIONS

The most common causes of division inoperability are outright failure or drift of the sensor sufficient to exceed the tolerance allowed by the plant specific setpoint analysis. Typically, the drift is found to be small and results in a delay of actuation rather than a total loss of function. This determination is generally made during the performance of a CALIBRATION when the sensor is set up for adjustment to bring it to within specification. If an as-found sensor calibration setting value is non-conservative with respect to the Allowable Value, the sensor is immediately declared inoperable, and the appropriate Condition(s) must be entered.

In the event that any sensor or function processor is found inoperable, then all affected Trip/ESF/Permissive Functions provided by that sensor or function processor must be declared inoperable, and the plant must enter any applicable Condition for the particular Trip/ESF/Permissive Function affected.

When the number of inoperable Functions exceeds that specified in Table 3.3.1-1, redundancy is lost and actions must be taken to restore the required redundancy.

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

BASES

ACTIONS (continued)

A.1

Condition A applies to all Reactor Trip Instrumentation Functions. Condition A addresses the situation where one or more Functions with one or more divisions are inoperable. The Required Action is to refer to Table 3.3.1-1 and to take the Required Actions for the Functions affected. The Completion Times are those from the referenced Conditions and Required Actions.

B.1

Condition B applies when one Input & Acquisition Logic division is inoperable. In this condition, the minimum number of OPERABLE divisions to read the plant parameter, perform conditioning, calculations, compare the values to setpoints, and sending to the voting logic during an AOO or postulated accident coupled with a single failure is still available. Verification that the Actuation Logic voting has been modified ensures the Protection System reflects the condition. The Completion Time of 6 hours is reasonable considering the availability of automatic actuation and the low probability of an AOO or postulated accident occurring during this time.

C.1

Condition C The Completion Time of applies when one Manual division is inoperable. In this condition, the remaining OPERABLE Manual divisions are available to send a trip signal during an AOO or postulated accident coupled with a single failure.

The OPERABILITY of the other Manual divisions must be verified within 6 hours. The Completion Time of 6 hours is reasonable considering that there are three Manual divisions available, the low probability of an event occurring during this interval and the time necessary for performing the verification.

BASES

ACTIONS (continued)

D.1

Condition D applies when two Manual divisions are inoperable. In this condition, the two remaining OPERABLE Manual divisions are available to send a trip signal during an AOO or postulated accident.

One inoperable Manual division must be restored to OPERABLE status within 72 hours. The Completion Time of 72 hours is reasonable considering that there are two Manual divisions available, the low probability of an event occurring during this interval, and the time necessary for repairs.

E.1

Condition E applies when one Reactor Trip Breaker or one Reactor Trip Contactor in a set is inoperable.

A Note has been added to the Condition to clarify the application of the Completion Time rules. The Conditions of this Specification may be entered independently for each Reactor Trip Contactor Set. The Completion Times of each inoperable Reactor Trip Contactor Set will be tracked separately, starting from the time the Condition was entered for that Reactor Trip Contactor Set.

In this condition, the remaining OPERABLE Reactor trip Breakers and Reactor Trip Contactors in the set are available to open the breakers during an AOO or postulated accident coupled with a single failure.

The operability of the Reactor Trip Breaker or Reactor Trip Contactor in a set must be restored to OPERABLE status within 72 hours. The Completion Time of 72 hours is reasonable considering the availability Reactor trip Breakers and Reactor Trip Contactors, the low probability of an event occurring during this interval, and the time necessary for repairs.

In this condition, the remaining OPERABLE Reactor trip Breakers and Reactor Trip Contactors in the set are available to open the breakers during an AOO or postulated accident coupled with a single failure.

BASES

ACTIONS (continued)

The operability of the Reactor Trip Breaker or Reactor Trip Contactor in a set must be restored to OPERABLE status within 72 hours. The Completion Time of 72 hours is reasonable considering the availability Reactor trip Breakers and Reactor Trip Contactors, the low probability of an event occurring during this interval, and the time necessary for repairs.

F.1

Condition F addresses the failure of two or more Input & Acquisition Logic divisions, or the inability to complete the remedial measures in the time allowed by Required Action B.1. The plant must be brought to a MODE where the LCO is no longer applicable.

The Completion Time of 4 hours to reach MODE 1 with P2 inhibited is reasonable, based on operating experience, to reach the required power level from full power conditions in an orderly manner and without challenging plant systems.

G.1

Condition G addresses the failure of two or more Input & Acquisition Logic divisions, three or more manual divisions, two or more Reactor Trip Breakers, two or more Reactor Trip Contactors in any set, or the inability to complete the remedial measures in the time allowed by Required Actions B.1, C.1, D.1, or E.1. The plant must be brought to a MODE where the LCO is no longer applicable.

The Completion Time of 6 hours to reach MODE 3 with the Reactor Control, Surveillance and Limitation (RCSL) System not capable of withdrawing an RCCA and RCCAs fully inserted is reasonable, based on operating experience, to reach the required power level from full power conditions in an orderly manner and without challenging plant systems.

H.1

Condition H addresses the failure of two or more Input & Acquisition Logic divisions or the inability to complete the remedial measures in the time allowed by Required Action B.1. The plant must be brought to a MODE where the LCO is no longer applicable.

BASES

ACTIONS (continued)

The Completion Time of 6 hours to reach MODE 2 with P5 inhibited is reasonable, based on operating experience, to reach the required power level from full power conditions in an orderly manner and without challenging plant systems.

I.1

Condition I addresses the failure of two or more Input & Acquisition Logic divisions or the inability to complete the remedial measures in the time allowed by Required Action B.1. The plant must be brought to a MODE where the LCO is no longer applicable.

The Completion Time of 6 hours to reach MODE 3 with the Reactor Control, Surveillance and Limitation (RCSL) System not capable of withdrawing an RCCA and RCCAs fully inserted with P12 validated is reasonable, based on operating experience, to reach the required power level from full power conditions in an orderly manner and without challenging plant systems.

J.1

Condition J addresses the failure of two or more Input & Acquisition Logic divisions or the inability to complete the remedial measures in the time allowed by Required Action B. The plant must be brought to a MODE where the LCO is no longer applicable.

The Completion Time of 6 hours to reach MODE 2 is reasonable, based on operating experience, to reach the required power level from full power conditions in an orderly manner and without challenging plant systems.

K.1

Condition K addresses the failure of two or more Input & Acquisition Logic divisions or the inability to complete the remedial measures in the time allowed by Required Action B.1. The plant must be brought to a MODE where the LCO is no longer applicable.

The Completion Time of 2 hours to reach MODE 1 with P3 inhibited is reasonable, based on operating experience, to reach the required power level from full power conditions in an orderly manner and without challenging plant systems.

BASES

ACTIONS (continued)

L.1

Condition L addresses the failure of two or more Input & Acquisition Logic divisions or the inability to complete the remedial measures in the time allowed by Required Action B.1. The plant must be brought to a MODE where the LCO is no longer applicable.

The Completion Time of 6 hours to reach MODE 3 is reasonable, based on operating experience, to reach the required power level from full power conditions in an orderly manner and without challenging plant systems.

M.1

Condition M applies when one Actuation Logic division is inoperable. In this condition, the minimum number of OPERABLE divisions to send the voting logic during an AOO or postulated accident coupled with a single failure is still available. The OPERABILITY of the other Actuation Logic division must be verified within 6 hours. The Completion Time of 6 hours is reasonable considering the low probability of an event occurring during this interval and the time necessary to perform the verification.

N.1, N.2, N.3, N.4, N.5, N.6, and N.7

Condition N addresses the failure of two or more Actuation Logic divisions or the inability to complete the remedial measures in the time allowed by Required Action M.1.

The Completion Time Required Action N.1 is modified by a Note that clarifies its applicability. Required Action N.1 is only applicable to the following Functions:

1. DNBR - Low,
2. DNBR with High Quality – Low,
3. DNBR with Imbalance or Rod Drop (1/4) – Low,
4. DNBR with High Quality and (Imbalance or Rod Drop) (1/4) - Low,
5. DNBR with Rod Drop (2/4) – Low,
6. Linear Power Density - High,
10. RCS Flow Rate – Low in Two Loops,
12. RCP Speed – Low in Two Loops, and
15. Pressurizer Pressure - Low.

BASES

ACTIONS (continued)

In this condition, the associated Functions are inoperable and the plant must be brought to a MODE where the associated LCO is no longer applicable. To achieve this status, the plant must be brought to at least MODE 1 with P2 inhibited within 4 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.

Required Action N.2 is modified by a Note that clarifies its applicability. Required Action N.2 is only applicable to the following Functions:

7. Neutron Flux Rate of Change - High,
13. Neutron Flux - High (Intermediate Range),
14. Doubling Time – Low,
19. SG Pressure Drop – High,
23. SG Level - High,
24. Containment Pressure - High, and
26. EFWS Actuation - Low-Low SG Level.

In this condition, the associated Functions are inoperable and the plant must be brought to a MODE where the associated LCO is no longer applicable. To achieve this status, the plant must be brought to at least MODE 3 with the RCSL not capable of withdrawing an RCCA and RCCAs fully inserted within 6 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.

Required Action N.3 is modified by a Note that clarifies its applicability. Required Action N.3 is only applicable to the following Functions:

8. Core Power Level – High, and
9. Saturation Margin - Low

In this condition, the associated Functions are inoperable and the plant must be brought to a MODE where the associated LCO is no longer applicable. To achieve this status, the plant must be brought to at least MODE 2 with P5 inhibited within 6 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.

BASES

ACTIONS (continued)

Required Action N.4 is modified by a Note that clarifies its applicability. Required Action N.4 is only applicable to the following Functions:

18. Hot Leg Pressure - Low, and
20. SG Pressure - Low.

In this condition, the associated Functions are inoperable and the plant must be brought to a MODE where the associated LCO is no longer applicable. To achieve this status, the plant must be brought to at least MODE 3 with P12 validated and the RCSL not capable of withdrawing an RCCA and RCCAs fully inserted within 6 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.

Required Action N.5 is modified by a Note that clarifies its applicability. Required Action N.5 is only applicable to the SG Pressure - High Function. In this condition, the Function is inoperable and the plant must be brought to a MODE where the associated LCO is no longer applicable. To achieve this status, the plant must be brought to at least MODE 2 within 6 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.

Required Action N.6 is modified by a Note that clarifies its applicability. Required Action N.6 is only applicable to the RCS Flow Rate – Low-Low in One Loop Function. In this condition, the Function is inoperable and the plant must be brought to a MODE where the associated LCO is no longer applicable. To achieve this status, the plant must be brought to at least MODE 3 with P3 inhibited within 6 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.

Required Action N.7 is modified by a Note that clarifies its applicability. Required Action N.7 is only applicable to the following Functions:

16. Pressurizer Pressure - High,
17. Pressurizer Level - High,
22. SG Level - Low, and
25. SI Actuation - Automatic.

BASES

ACTIONS (continued)

In this condition, the associated Functions are inoperable and the plant must be brought to a MODE where the associated LCO is no longer applicable. To achieve this status, the plant must be brought to at least MODE 3 within 6 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

The SRs for each Function are identified by the Surveillance Requirements (SR) column of Table 3.3.1-1 for that Function. Most Functions are subject to CHANNEL CHECK, ACTUATION DEVICE OPERATIONAL TEST, CALIBRATION, SENSOR OPERATIONAL TEST, EXTENDED SELF TESTS, and RESPONSE TIME testing.

The SRs are modified by a Note. The Note directs the reader to Table 3.3.1-1 to determine the correct SRs to perform for each Function.

SR 3.3.1.1

SR 3.3.3.1 compares the calorimetric heat balance calculation to the Power Range Detector division output every 24 hours. If the calorimetric heat balance calculation results exceed the Power Range Detector division output by more than 2% RTP, the Power Range Detector division is not declared inoperable, but must be adjusted. The Power Range Detector division output shall be adjusted consistent with the calorimetric heat balance calculation results if the calorimetric calculation exceed the Power Range Detector division output by more than +2% RTP. If the Power Range Detector division output cannot be properly adjusted, the division is declared inoperable.

If the calorimetric is performed at reduced power (< 70% RTP), adjusting the Power Range Detector division output in the increasing power direction will assure a reactor trip below the safety analysis limit (< 117% RTP). Making no adjustment to the Power Range Detector division output in the decreasing power direction due to a reduced power calorimetric assures a reactor trip consistent with the safety analyses.

BASES

SURVEILLANCE REQUIREMENTS (continued)

This allowance does not preclude making indicated power adjustments, if desired, when the calorimetric heat balance calculation is less than the Power Range Detector division output. To provide close agreement between indicated power and to preserve operating margin, the Power Range Detector division outputs are normally adjusted when operating at or near full power during steady-state conditions. However, discretion must be exercised if the Power Range Detector division output is adjusted in the decreasing power direction due to a reduced power calorimetric (< 70% RTP).

This action may introduce a non-conservative bias at higher power levels. The cause of the potential non-conservative bias is the decreased accuracy of the calorimetric at reduced power conditions. The primary error contributor to the instrument uncertainty for a secondary side power calorimetric measurement is the feedwater flow measurement, which is typically a delta pressure measurement across a feedwater venturi.

While the measurement uncertainty remains constant in delta pressure as power decreases, when translated into flow, the uncertainty increases as a square term. Thus a 1% flow error at 100% power can approach a 10% flow error at 30% RTP even though the delta pressure error has not changed.

An evaluation of extended operation at reduced power conditions would conclude that it is prudent to administratively adjust the setpoint of the High Neutron Flux Rate of Change (Power Range) reactor trip when: 1) the Power Range Detector division output is adjusted in the decreasing power direction due to a reduced power calorimetric below 70% RTP; or 2) for a post refueling startup. The evaluation of extended operation at reduced power conditions would also conclude that the potential need to adjust the setpoint of the High Neutron Flux Rate of Change (Power Range) reactor trip in the decreasing power direction is quite small, primarily to address operation in the intermediate range about 10% RTP to allow enabling of the High Neutron Flux Rate of Change (Power Range) reactor trips. Before the High Neutron Flux Rate of Change (Power Range) reactor trip setpoint is reset, the Power Range Detector division output adjustment must be confirmed based on a calorimetric performed at ≥ 70% RTP.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The Note clarifies that 12 hours are allowed for performing the first Surveillance after reaching 20% RTP. A reactor power level of 20% RTP is chosen based on plant stability, (i.e., automatic rod control capability and turbine generator synchronized to the grid). The Frequency of every 24 hours is adequate. It is based on plant operating experience, considering instrument reliability and operating history data for instrument drift. Together these factors demonstrate that a difference between the calorimetric heat balance calculation and the Power Range Detector division output of more than +2% RTP is not expected in any 24 hour period.

SR 3.3.1.2

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

Agreement criteria are determined by the plant staff, based on a combination of the channel instrument uncertainties, including isolation, indication, and readability. If a channel is outside the criteria, it may be an indication that the sensor or the signal processing equipment has drifted outside its limit. If the channels are within the criteria, it is an indication that the channels are OPERABLE.

The Frequency of 31 days is based on operating experience that demonstrates that channel failure is rare. The CHANNEL CHECK supplements less formal checks of channels during operational use of the displays associated with the LCO required channels.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.1.3

SR 3.3.1.3 is the performance of an ADOT every 31 days. This test shall verify OPERABILITY by actuation of the RTBs and RTCs. The ADOT may be performed by means of any series of sequential, overlapping, or total steps.

SR 3.3.1.4

The incore – excore CALIBRATION for the Power Range indication consists of a normalization of the detector addressable constant multipliers based on a power calorimetric and flux map performed at or above 15% RTP. This surveillance is modified by two Notes. The first Note to the SR states that the SR is not required to be performed until 24 hours after THERMAL POWER ≥ 15% RTP. At lower power levels, incore – excore calibration of the Power Range Detectors would be

inaccurate. During a refueling startup calibrations performed at lower power levels should be verified against higher level flux maps and calibrated, if necessary, to ensure accurate power range performance. The second Note states that neutron detectors are excluded from the CALIBRATION. The CALIBRATION for the Source Range Detectors consists of obtaining the detector plateau or preamp discriminator curves, evaluating those curves, and comparing the curves to the manufacturer's data. This Surveillance is not required for the Intermediate Range Detectors for entry into MODE 2, because the plant must be in at least MODE 2 to perform the test for the Intermediate Range Detectors.

If the absolute difference between the power range and incore measurements is greater than the allowable difference specified in the Setpoint Control Program, the power range channel is not inoperable, but an adjustment of the addressable constant multipliers is necessary to ensure that the incore measured axial offset agrees with the indicated excore axial offset. If the power range channel cannot be properly recalibrated, the channel is declared inoperable. The 31 day Frequency is adequate, considering that long term drift of the excore linear amplifiers is small, burnup of the detectors, and changes in axial offset are slow. Also, the excore readings are a strong function of the power produced in the peripheral fuel bundles, and do not represent an integrated reading across the core. The slow changes in neutron flux during the fuel cycle (radially and axially) can also be detected and incorporated in the periodic incore – excore CALIBRATION at this interval.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.1.5

A CALIBRATION of each RCS flow indication and calculation input every 24 months ensures that each instrument division is accurate and within the specified tolerance. This CALIBRATION consists of a normalization of the addressable constant multipliers based on RCS flow measured by a precision calorimetric (SR 3.4.1.4). If the absolute difference between the flow indication / calculation input and the value measured in the surveillance is greater than the allowable difference specified in the Setpoint Control Program, the flow indication / calculation input are not inoperable, but an adjustment of the addressable constant multipliers is necessary to ensure that the flow indication / calculation input agrees with measured RCS flow. If the RCS flow indication and calculation input cannot be properly recalibrated, the division is declared inoperable.

The Note to the SR states that the CALIBRATION is not required to be performed until 12 hours after THERMAL POWER ≥ 70% RTP. The RCS Flow Rate – Low-Low in One Loop trip function is required to be OPERABLE in MODE 1 with P3 permissive validated, which corresponds to this power level. The 24 month Frequency is adequate, considering that the RCS flow change over an operating cycle is small.

SR 3.3.1.6

A SENSOR OPERATIONAL TEST (SOT) is performed every 24 months to ensure the devices will perform their intended function when needed. The test is performed in accordance with the Setpoint Control Program. A SOT shall be the injection of a simulated or actual signal into the division as close to the sensor as practicable to verify OPERABILITY of all devices in the division required for division OPERABILITY. The SOT shall include the verification of the accuracy and time constants of the analog input modules.

The SOT may be performed by means of any series of sequential, overlapping, or total steps.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.1.7

A CALIBRATION of each sensor every 24 months ensures that each instrument division is reading accurately and within tolerance. The test is performed in accordance with the Setpoint Control Program. A CALIBRATION shall be the adjustment, as necessary, of the sensor output such that it responds within the necessary range and accuracy to known values of the parameter that the division monitors. The CALIBRATION shall encompass all devices in the division required for sensor OPERABILITY.

The CALIBRATION includes provisions for the following:

1. Evaluation of sensor performance to verify that the sensor is functioning as required prior to returning the sensor to service if the as-found sensor calibration setting values are outside their predefined as-found tolerance for the specified calibration settings (e.g., 0, 25, 50, 75, and 100 percent), but conservative with respect to the Allowable Value, and

2. Declaring the sensor immediately inoperable if the sensor cannot be calibrated such that the as-left sensor calibration setting values are within the specified as-left tolerance around the specified calibration settings (e.g., 0, 25, 50, 75, and 100 percent), at the completion of the surveillance.

The CALIBRATION may be performed by means of any series of sequential, overlapping, or total steps.

SR 3.3.1.8

The features of continuous self-monitoring of the Protection System are described in Reference 8. Additional tests, which require the function processor to be inoperable are not normally performed during operation. These EXTENDED SELF TESTS are performed at start-up of a function processor each cycle. The startup sequence is as follows:

– Hardware basic test using the internal diagnosis monitor,
– Start-up self-test of the operating system, and
– Switch over to normal operation after approximately two minutes.

Additional information is provided in Section 2 of Reference 8.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.1.9

SR 3.3.1.9 is the performance of an ACTUATING DEVICE OPERATIONAL TEST (ADOT) every 24 months. The ADOT may be performed by means of any series of sequential, overlapping, or total steps.

SR 3.3.1.10

SR 3.3.1.10 verifies that the NTSPs have been properly loaded into the applicable APUs.

SR 3.3.1.11

Instrument Calibration

For intermediate range neutron flux channels, CALIBRATION is a complete check and readjustment of the channels, from the preamplifier input to the indicators. This test verifies the channel responds to a measured parameter within the necessary range and accuracy. CALIBRATION leaves the channel adjusted to account for instrument drift to ensure that the instrument channel remains operational between successive tests. There is a plant specific program which verifies that the instrument channel functions as required by verifying the as-left and as-found settings are consistent with those established by the setpoint methodology.

Setpoint Determination

Before each refueling startup determine the relative change in the peripheral assemblies when compared to the last time that the intermediate range setpoint (amps) was verified at the corresponding core power (percent power). Using the relative change for each assembly apply a weighting factor for a limited number of assemblies to calculate a new setpoint. The limited number of assemblies and the appropriate weighting factor is determined by a statistical analysis method (Monte Carlo). The analytical method determines the probability of a neutron that is born in any assembly reaching the intermediate range detector. For some assemblies like the center assembly in the core it is impossible to be born and survive long enough to get to the intermediate range detector. The setpoint calculation shall also account for things like replacing the detectors with a more sensitive model and changes in plant parameters, if necessary. During each startup (refueling or mid-cycle) the

BASES

SURVEILLANCE REQUIREMENTS (continued)

setpoint is verified when core power is equivalent to the intermediate range setpoint. If the absolute difference between the current intermediate range setpoint and the intermediate range current at the corresponding core power is greater than the allowable difference specified in the Setpoint Control Program, the intermediate range channel is not inoperable, but an adjustment of the addressable constant multipliers is necessary to ensure that the intermediate range measured current agrees with the desired intermediate setpoint. If the intermediate range channel cannot be properly recalibrated, the channel is declared inoperable. This intermediate range information can be used to make an adjustment to the setpoint, if necessary, and shall be used to calculate the next refueling setpoint.

General

The SR is modified by two Notes. The first Note requires the SR to be performed prior to withdrawing RCCAs for startup. The second Note excluding neutron detectors from CALIBRATION. It is not necessary to test the detectors because generating a meaningful test signal is difficult. In addition, the detectors are of simple construction, and any failures in the detectors will be apparent as a change in channel output. The Frequency is based on operating experience and consistency with the typical industry refueling cycle and is justified by demonstrated instrument reliability over a 24 month interval such that the instrument is not adversely affected by drift.

SR 3.3.1.12

This surveillance verifies that the individual division actuation response times are less than or equal to the maximum values assumed in the accident analysis. Response time testing acceptance criteria are included in a document controlled under 10 CFR 50.59. Individual component response times are not modeled in the analyses.

The analyses model the overall or total elapsed time, from the point at which the parameter exceeds the trip setpoint value at the sensor to the point at which the equipment reaches the required functional state (e.g., valves in full closed position).

For divisions that include dynamic transfer functions (e.g., lag, lead/lag, rate/lag, etc.), the response time test may be performed with the transfer function set to one, with the resulting measured response time compared to the appropriate FSAR response time. Alternately, the response time test can be performed with the time constants set to their nominal value,

BASES

SURVEILLANCE REQUIREMENTS (continued)

provided the required response time is analytically calculated assuming the time constants are set at their nominal values. The response time may be measured by a series of overlapping tests such that the entire response time is measured.

SR 3.3.1.12 is modified by a Note stating that neutron detectors are excluded from RTS RESPONSE TIME testing. This Note is necessary because of the difficulty in generating an appropriate detector input signal. Excluding the detectors is acceptable because the principles of detector operation ensure a virtually instantaneous response.

----------REVIEWER'S NOTE----------
The following Bases apply to plants that have obtained NRC approval to utilize allocations for selected components based on NRC-approved U.S. EPR-applicable Topical Reports.

[Response time may be verified by actual response time tests in any series of sequential, overlapping or total division measurements, or by the summation of allocated sensor, signal processing and actuation logic response times with actual response time tests on the remainder of the division. Allocations for sensor response times may be obtained from: (1) historical records based on acceptable response time tests (hydraulic, noise, or power interrupt tests), (2) in place, onsite, or offsite (e.g., vendor) test measurements, or (3) utilizing vendor engineering specifications. NRC-approved U.S. EPR-applicable Topical Report provides the basis and methodology for using allocated sensor response times in the overall verification of the division response time for specific sensors identified in the report. Response time verification for other sensor types must be demonstrated by test.

NRC-approved U.S. EPR-applicable Topical Report (provide reference) provides the basis and methodology for using allocated signal processing and actuation logic response times in the overall verification of the DCS division response time.

The allocations for sensor, signal conditioning, and actuation logic response times must be verified prior to placing the component in operational service and re-verified following maintenance that may adversely affect response time. In general, electrical repair work does not impact response time provided the parts used for repair are of the same type and value. One example where response time could be affected is replacing the sensing assembly of a transmitter.]

BASES

SURVEILLANCE REQUIREMENTS (continued)

As appropriate, each division's response must be verified every 24 months on a STAGGERED TEST BASIS. Testing of the final actuation devices is included in the testing. Response times cannot be determined during plant operation because equipment operation is required to measure response times. Experience has shown that these components usually pass this surveillance when performed at the 24 month Frequency. Therefore, the Frequency was concluded to be acceptable from a reliability standpoint.

REFERENCES

1. FSAR Section 7.1
2. 10 CFR 50, Appendix A, GDC 21.
3. 10 CFR 50.49.
4. ANP-10275P-A, "U.S. EPR Instrument Setpoint Methodology Topical Report," January 2008.
5. FSAR Chapter 15.
6. 10 CFR 100.
7. ANP-10287P, Revision 1, "Incore Trip Setpoint and Transient Methodology for U.S. EPR Topical Report," April 2012.
8. ANP-10315P, Revision 1, "U.S. EPR Protection System Surveillance Testing and Teleperm XS Self-Monitoring Technical Report," June 2011.

B 3.3 INSTRUMENTATION

B 3.3.2 Engineered Safety Feature Actuation System (ESFAS) Instrumentation

BASES

BACKGROUND

Refer to B 3.3.1, “Reactor Trip Instrumentation,” for background information on the Distributed Control System.

The Engineered Safety Feature (ESF) function logic monitors plant conditions and initiates the operation of necessary features in response to accident situations. The ESF functions along with reactor trips ensure the following:

– The integrity of the reactor coolant pressure boundary;

– The capability to shut down the reactor and maintain it in a safe shutdown condition; and

– The capability to prevent or mitigate the consequences of accidents which could result in potential off-site exposures.

As with the reactor trip logic, critical plant parameters such as temperatures, pressures, and levels are sensed, acquired, and converted to electrical signals by the Signal Conditioning and Distribution System (SCDS) and acquired by the PS. When prohibited operating conditions exist, an ESF actuation signal is generated from the PS. In addition to the automatic ESF functions performed by the PS, the capability to manually initiate these functions is provided in the main control room. These manual functions are implemented at the system level and perform the same actions as the automatic functions.

Single failures upstream of the Actuation Logic Units (ALU) layer that could result in an invalid signal being used in the ESF function are accommodated by modifying the vote in the ALU layer. Each ESF function is evaluated on a case-by-case basis to determine whether the vote is modified toward actuation or no actuation. In cases where inappropriate actuation of an ESF function could challenge plant safety, the function is modified toward no actuation. Otherwise, the function is modified toward actuation.

The ESF actuation signals of the redundant ALUs in each subsystem are combined in a hardwired “functional OR” logic; therefore, either of the redundant ALUs in a subsystem can actuate an ESF function.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

The Distributed Control System (DCS) is designed to ensure that the following operational criteria are met:

– The associated actuation will occur when the parameter monitored by each division reaches its setpoint and the specific coincidence logic is satisfied; and

– In general, separation and redundancy are maintained to permit a division to be out of service for testing or maintenance while still maintaining redundancy within the DCS instrumentation network.

Each of the analyzed transients and accidents can be detected by one or more PS functions. Each of the automatic ESFAS actuations included in the Technical Specifications are credited as part of the primary success path in the accident analysis. Therefore, the automatic ESFAS Instrumentation satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii). Refer to FSAR Sections 7.3 for a description of the ESF functions. Credited functions are included in FSAR Tables 15.0-8 and 15.0-9. Manual initiation of ESFAS Functions satisfies Criterion 4 of 10 CFR 50.36(c)(2)(ii). Exception are noted when the manual Function is credited as part of the safety analysis (Ref. 1).

In general, the Input & Acquisition Logic Divisions, Actuation Logic Divisions, Manual Divisions, and actuated devices that support reactor trips are required to be OPERABLE in MODES 1, 2 and/or 3 because the reactor is or can be made critical in these MODES. The automatic reactor trip functions are designed to take the reactor subcritical, which maintains the Safety Limits (SL) during AOOs and assists the ESF in providing acceptable consequences during accidents. The Input & Acquisition Logic Divisions, Actuation Logic Divisions, Manual Divisions, and actuated devices that support reactor trip functions are not required to be OPERABLE in MODES 4 and 5 when all RCCAs are fully inserted, and only if the Reactor Control, Surveillance and Limitation (RCSL) System is placed in a configuration whereby inadvertent RCCA withdrawal is precluded. In MODES 4 and 5, the emphasis is placed on return to power events. The reactor is protected in these MODES by ensuring adequate shutdown margin (SDM).

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

In general, the Input & Acquisition Logic Divisions, Actuation Logic Divisions, Manual Divisions, and actuated devices that support ESFAS functions are required to be OPERABLE in MODES 1, 2, 3 and/or 4 since there is sufficient energy in the primary and secondary systems to warrant automatic ESF system responses to:

- Isolate the Main Steam System to preclude a positive reactivity addition,
- Actuate the Emergency Feedwater System (EFWS) to preclude the loss of the steam generators (SG) as a heat sink (in the event the normal feedwater system is not available),
- Actuate ESF systems to prevent or limit the release of fission product radioactivity to the environment by isolating containment and limiting the containment pressure from exceeding the containment design pressure during a design basis Loss of Coolant Accident (LOCA) or Main Steam Line Break (MSLB), and
- Actuate ESF systems to ensure sufficient borated inventory to permit adequate core cooling and reactivity control during a design basis LOCA or MSLB accident.

In MODES 5 and 6, automatic actuation of ESF functions is not normally required because adequate time is available to evaluate plant conditions and respond by manually operating the ESF components if required. Exceptions to this are:

- ESF 1.c: SIS Actuation - Low Hot Leg Loop Level,
- ESF 11.a: Pressure Safety Relief Valve (PSRV) Opening – High Hot Leg Pressure,
- Chemical and Volume Control System Isolation (Refer to LCO 3.3.5, “Chemical and Volume Control System (CVCS) Isolation Instrumentation,”)
- Control Room Emergency Filtration (Refer to LCO 3.3.7, “Control Room emergency Filtration (CREF) Instrumentation,”) and
- EDG Actuation (Refer to LCO 3.3.8, “EDG Actuation Instrumentation,”).

These ESF functions are required to be OPERABLE in MODES 5 and 6, and during movement of irradiated fuel assemblies to ensure that:

- Systems to provide adequate coolant inventory makeup are available for the irradiated fuel assemblies in the core;
- Systems needed to mitigate a fuel handling accident are available; and
- Systems necessary to mitigate the effects of events that can lead to core damage during shutdown are available.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

The specific safety analysis and OPERABILITY requirements applicable to each protective function are identified below. Permissives that enable a credited function are included in the Technical Specifications.

LCO 3.3.2, “Engineered Safety Feature Actuation System (ESFAS) Instrumentation,” addresses the following Functions:

1. Safety Injection System (SIS) Actuation

a. SIS Actuation - Low Pressurizer Pressure

In the event of a decrease in RCS water inventory, the makeup is supplied by the Medium Head Safety Injection (MHSI) in the high pressure phase of the event and the Low Head Safety Injection (LHSI) in the low pressure phase. For a potential overcooling event, the reactivity insertion is limited by the boron injection via the MHSI. Even if the boron injection is not required, MHSI injection is needed to stabilize the RCS pressure. This Function mitigates the following postulated accidents or AOOs:

– Excessive increase in secondary steam flow,
– Steam Generator Tube Rupture (SGRT),
– Small break LOCA,
– Inadvertent opening of a pressurizer pilot operated safety valve,
– MSLB,
– Large break LOCA.

Four divisions of the SIS Actuation - Low Pressurizer Pressure Function are required to be OPERABLE in:

– MODES 1, 2, and
– MODE 3 with P12 permissive inhibited.

This Function utilizes the Pressurizer Pressure (Narrow Range) sensors.

The NTSP is sufficiently below the full load operating value for RCS pressure so as not to interfere with normal plant operation. However, the NTSP is high enough to provide an SIS actuation during an RCS depressurization.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

Inhibition of the P12 permissive automatically enables the SIS Actuation - Low Pressurizer Pressure Function when the pressurizer pressure is greater than or equal to approximately 2005 psia. When below this threshold, the Function is disabled by manual validation of the P12 permissive.

b. SIS Actuation - Low Delta P_{sat}

In case of the listed events, this Function ensures that the SIS actuates before saturation occurs in a hot leg. This Function mitigates the following postulated accidents or AOOs:

– Small break LOCA,
– Large break LOCA, and
– Inadvertent opening of a pressurizer pilot operated safety valve.

– Four divisions of the SIS Actuation - Low Delta P_{sat} Function are required to be OPERABLE in MODE 3. Three divisions are required to be OPERABLE in MODE 4 with P12 permissive validated and P15 permissive inhibited.

– This Function utilizes the Hot Leg Pressure (Wide Range) and Hot Leg Temperature (Wide Range) sensors.

– The NTSP is low enough to avoid spurious operation but high enough to maintain core coverage in the event of an RCS pipe break.

– Manual validation of the P12 permissive enables the SIS Actuation - Low Delta P_{sat} Function when the pressurizer pressure is less than approximately 2005 psia. Manual validation of the P15 permissive disables the SIS Actuation - Low Delta P_{sat} Function when no RCPs are running, the hot leg pressure is less than approximately 464 psia, and the hot leg temperature is less than approximately 350ºF.

– For loss of RHR scenarios with RCPs running, the RCS inventory would be essentially full with the pressurizer at normal level. The secondary side (steam generator) would also be available if RCPs were in operation. Under these conditions, a loss of RHR event

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

would result in a minor heat-up until decay heat is removed through the secondary side. Thus, safety injection on Low Delta P_{sat} would not be required in MODE 5 if RCPs were in operation, but would still be available.

c. SIS Actuation - Low Hot Leg Loop Level

This Function mitigates the following postulated accidents or AOOs:

– Loss of Residual Heat Removal during mid-loop operations,
– Uncontrolled loss of RCS inventory,
– Small break LOCA, and
– Large break LOCA.

Three divisions of the SIS Actuation - Low Hot Leg Loop Level Function are required to be OPERABLE in MODE 4 with P15 permissive validated and Manual SIS – Loop Level Bypass inhibited. Two divisions of the SIS Actuation - Low Hot Leg Loop Level Function are required to be OPERABLE in MODES 5 and 6 with P15 permissive validated and Manual SIS – Loop Level Bypass inhibited.

This Function utilizes the Hot Leg Loop Level sensors.

The NTSP is low enough to avoid spurious operation but high enough to ensure core cooling is maintained.

In MODES 5 and 6, safety injection requirements are based on loss of RHR events during reduced inventory (mid-loop) conditions. Before entering mid-loop operation the RCPs are secured and the RCS is vented. Two MHSI pumps are available and automatic injection is available on low loop level following manual validation of the P15 permissive. In the event of a loss of RHR under these conditions, the MHSI pumps would automatically inject on low loop level to maintain the core covered and replace the inventory that boils-off.

Manual validation of the P15 permissive enables the SIS Actuation - Low Hot Leg Loop Level Function when no RCPs are running, the hot leg pressure is less than approximately 464 psia, and the hot leg temperature is less than approximately 350ºF.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

d. SIS Actuation - Manual

The capability for manual system-level initiation of the SIS is provided to the operator on the Safety Information and Control System (SICS) in the MCR. This manual system-level initiation starts the four trains of safety injection as well as the associated protective actions, such as partial cooldown and reactor trip. For a SGTR event, the operator is credited to perform a manual system-level initiation of SIS from the SICS. Four manual system level initiation controls are provided, any two of which will start the four SIS trains.

This Function mitigates the following postulated accidents or AOOs:

– Excessive increase in secondary steam flow,
– SGTR,
– Small break LOCA,
– Inadvertent opening of a pressurizer pilot operated safety valve,
– MSLB,
– Large break LOCA.
– Loss of Residual Heat Removal during mid-loop operations, and
– Uncontrolled loss of RCS inventory.

Four divisions of this Function are required to be OPERABLE in MODES 1, 2, and 3. Three divisions are required to be OPERABLE in MODE and 4. Two divisions are required to be OPERABLE in MODES 5 and 6.

There is no NTSP associated with this Function.

There are no permissives associated with this Function.

The manual system-level initiation satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

2. Emergency Feedwater System (EFWS) Actuation

a. EFWS Actuation - Low-Low SG Level (Affected SG)

In case of loss of Main Feedwater (MFW), the EFWS is actuated to remove residual heat via secondary side. With an EFWS actuation signal, SG blowdown is also isolated to conserve SG inventory. This Function ensures heat is removed from the primary system through the SGs in the event of a loss of MFW or feedwater line break, as indicated by low SG level.

This Function mitigates the following postulated accidents or AOOs:

– Loss of normal feedwater flow,
– Feedwater system piping failure, and
– Loss of Offsite Power (LOOP).

Four divisions of the EFWS Actuation - Low-Low SG Level (Affected SG) Function are required to be OPERABLE in:

– MODES 1 and 2, and
– MODE 3 with P13 permissive inhibited.

This Function utilizes the SG Level (Wide Range) and SG Pressure sensors.

The NTSP is low enough to provide an operating envelope that prevents unnecessary actuations but high enough to ensure sufficient make-up is provided to the SGs.

Inhibition of the P13 permissive automatically enables the EFWS Actuation - Low-Low SG Level Function when the hot leg temperature is greater than or equal to approximately 200°F. When below this threshold, the Function is disabled by manual validation of the P13 permissive.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

b. EFWS Actuation - Manual (Affected SG)

The capability for manual system-level initiation of the EFWS on a per-train basis is provided on the SICS in the MCR. Three manual system-level initiation controls are provided per EFW train. One-out-of-two logic is used on two of these controls to start the EFW pump, open the associated EFW valves, and isolate the SG blowdown line. The third control is used only to close SG blowdown isolation valves that are redundant to those closed by the first two controls.

This Function mitigates the following postulated accidents or AOOs:

– Loss of normal feedwater flow,
– Feedwater system piping failure, and
– Loss of Offsite Power (LOOP).

Four divisions of the EFWS Actuation – Manual (Affected SG) Function are required to be OPERABLE in MODES 1, 2, and 3. Two divisions of the EFWS Actuation – Manual (Affected SG) Function are required to be OPERABLE in MODE 4 with P13 permissive inhibited and the SGs are relied upon for heat removal.

There is no NTSP associated with this Function.

Inhibition of the P13 permissive automatically enables the EFWS Actuation - Manual Function when the hot leg temperature is greater than or equal to approximately 200°F. When below this threshold, the Function is disabled by manual validation of the P13 permissive.

3. Common Steam Generator Blowdown (SGBD) Valve Isolation

a. Common SGBD Valve Isolation - Manual

The capability for manual system-level initiation of the EFWS (which includes SGBT valve isolation) on a per-train basis is provided on the SICS in the MCR. Three manual system-level initiation controls are provided per EFW train. One-out-of-two logic is used on two of these controls to start the EFW pump, open the associated EFW valves, and isolate the SG blowdown line. The third control is used only to close SG blowdown isolation valves that are redundant to those closed by the first two controls.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

In case of loss of MFW, the EFWS is actuated to remove residual heat via secondary side. With an EFWS actuation signal, SG blowdown is also isolated to conserve SG inventory. This Function ensures heat is removed from the primary system through the SGs in the event of a loss of MFW or feedwater line break, as indicated by low SG level.

The capability for manual system-level initiation of SG isolation (which includes SGBT valve isolation) on a per SG basis is provided on the SICS in the MCR. Four manual system-level initiation controls are provided per SG, any two of which will isolate the desired SG.

In case of an SGTR, partial cooldown is initiated to depressurize the RCS to the point where MHSI becomes effective. The SG containing the tube rupture is isolated after the partial cooldown is initiated if a high SG level or high main steam activity level is detected. This is done to prevent the release of contaminated fluid from the affected SG, and to prevent other water sources from adding to the uncontrolled SG level increase.

Two divisions of the Common SGBD Valve Isolation - Manual Function are required to be OPERABLE in MODES 1, 2, and 3 and in MODE 4 with P13 permissive inhibited and the SGs are relied upon for heat removal.

There is no NTSP associated with this Function.

Inhibition of the P13 permissive automatically enables the Common SGBD Valve Isolation - Manual Function when the hot leg temperature is greater than or equal to approximately 200°F. When below this threshold, the Function is disabled by manual validation of the P13 permissive.

4. EFWS Isolation

a. EFWS Isolation - High SG Level (Affected SG)

In case of a SGTR, the EFWS is isolated to avoid SG overfill and potential radioactive water discharge via the main steam relief train.

This Function mitigates a SGTR.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

Four divisions of the EFWS Isolation - High SG Level (Affected SG) Function are required to be OPERABLE in:

– MODES 1 and 2, and
– MODE 3 with P13 permissive inhibited.

This Function utilizes the SG Level (Wide Range) and SG Pressure sensors.

The NTSP is high enough to provide an operating envelope that prevents unnecessary isolations but low enough to ensure sufficient make-up is provided to the SGs.

Inhibition of the P13 permissive automatically enables the EFWS Isolation on High SG Level Function when the hot leg temperature is greater than or equal to approximately 200°F. When below this threshold, the Function is disabled by manual validation of the P13 permissive.

b. EFWS Isolation - Manual

The capability for manual system-level EFWS isolation on a per train basis is provided to the operator on the SICS in the MCR. Two manual system-level isolation controls are provided per EFWS train. Any one of these two controls actuates the isolation function.

In case of a SGTR, the EFWS is manually isolated to avoid SG overfill and potential radioactive water discharge via the main steam relief train.

This Function mitigates a SGTR.

Four divisions of the EFWS Isolation – Manual (Affected SG) Function are required to be OPERABLE in MODES 1, 2, and 3 and in MODE 4 with P13 permissive inhibited and the SGs are relied upon for heat removal.

There is no NTSP associated with this Function.

Inhibition of the P13 permissive automatically enables the EFWS Isolation - Manual Function when the hot leg temperature is greater than or equal to approximately 200°F. When below this threshold, the Function is disabled by manual validation of the P13 permissive.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

Inhibition of the P13 permissive automatically enables the EFWS Isolation - Manual Function when the hot leg temperature is greater than or equal to approximately 200°F. When below this threshold, the Function is disabled by manual validation of the P13 permissive.

5. Partial Cooldown Actuation

a. Partial Cooldown Actuation – Automatic on SIS Actuation

The partial cooldown consists of lowering the main steam relief isolation valve (MSRIV) opening setpoint to allow depressurization of the RCS to a point where the MHSI is effective.

This Function mitigates the following postulated accidents or AOOs:

– Excessive increase in secondary steam flow,
– MSLB,
– Inadvertent opening of a Pressurizer pilot operated safety valve,
– SGTR, and
– Small break LOCA.

Four divisions of the Partial Cooldown Actuation – Automatic on SIS Actuation Function are required to be OPERABLE in MODES 1 and 2, and in MODE 3 with P14 permissive inhibited.

The sensors and NTSPs associated with this Function are described above for each individual automatic SIS Actuation Function (i.e., 1.a, 1.b, and 1.c).

Manual inhibition of the P14 permissive enables the Partial Cooldown Actuation – Automatic on SIS Actuation Function when the hot leg pressure is greater than or equal to approximately 464 psia or the hot leg temperature is greater than or equal to approximately 350°F. Manual validation of the P14 permissive disables the Function when the hot leg pressure is less than approximately 464 psia and the hot leg temperature is less than approximately 350°F.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

b. Partial Cooldown Actuation – Manual

The capability for manual system-level actuation of partial cooldown is provided on the SICS in the MCR. This manual initiation starts the partial cooldown via all four main steam trains if P14 is inhibited and the reactor is tripped. Four manual initiation controls are provided, any two of which will start the partial cooldown.

This Function mitigates the following postulated accidents or AOOs:

– Excessive increase in secondary steam flow,
– MSLB,
– Inadvertent opening of a Pressurizer pilot operated safety valve,
– SGTR, and
– Small break LOCA.

Four divisions of the Partial Cooldown Actuation – Manual Function are required to be OPERABLE in MODES 1, 2, and 3 and in MODE 4 with P14 permissive inhibited and the SGs are relied upon for heat removal.

There is no NTSP associated with this Function.

Manual inhibition of the P14 permissive enables the Partial Cooldown Actuation - Manual Function when the hot leg pressure is greater than or equal to approximately 464 psia or the hot leg temperature is greater than or equal to approximately 350°F. Manual validation of the P14 permissive disables the Function when the hot leg pressure is less than approximately 464 psia and the hot leg temperature is less than approximately 350°F.

6. Main Steam Relief Isolation Valve Opening

a. Main Steam Relief Isolation Valve (MSRIV) Opening– High SG Pressure (Affected SG)

In the event of a loss of the secondary side heat sink, the residual heat is removed through the steam relief valves to the atmosphere. This is done by the Main Steam Relief Train (MSRT). The MSRT also ensures SG overpressure protection, minimizes the actuation of the Main Steam Safety Valves (MSSV), which reduces the risk of a stuck open safety valve.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

This Function mitigates the following postulated accidents or AOOs:

– Total loss of load and/or turbine trip,
– Loss of main heat sink (condenser),
– Inadvertent closure of a Main Steam Isolation Valve (MSIV),
– SGTR,
– RCP seizure (locked rotor) or RCP shaft break, and
– Feedwater system piping failure.

Four divisions of the MSRIV Opening - High SG Pressure (Affected SG) Function are required to be OPERABLE in:

– MODES 1, 2, 3, and
– MODE 4 when the SGs are relied upon for heat removal.

This Function utilizes the following sensors:

– SG Pressure sensors,
– Hot Leg Temperature (Wide Range) sensors (for setpoint selection), and
– Hot Leg Pressure (Wide Range) sensors (for setpoint selection).

The NTSP is high enough to avoid spurious operation and low enough to open and relieve SG pressure before overpressurization limits are reached.

The P14 permissive is utilized for setpoint selection.

b. Partial Cooldown Actuation – Manual Reset

The capability for manual system-level reset of the Partial Cooldown Function is provided to the operator on the SICS in the MCR. This manual system-level reset enables the Partial Cooldown Actuation – Manual Function. Four manual system level initiation controls are provided, any one will reset its associated division.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

This Function mitigates the following postulated accidents or AOOs:

– Excessive increase in secondary steam flow,
– MSLB,
– Inadvertent opening of a Pressurizer pilot operated safety valve,
– SGTR, and
– Small break LOCA.

Four divisions of the Partial Cooldown Reset – Manual Function are required to be OPERABLE in MODES 1, 2, and 3.

There is no NTSP associated with this Function.

There are no permissives associated with this Function.

c. MSRIV Opening– Manual

The capability for manual system-level opening of the MSRIV on a per-train basis is provided on the SICS in the MCR. Two manual system-level initiation controls are provided per MSRIV. Any one of these two controls opens the desired MSRIV.

This Function mitigates the following postulated accidents or AOOs:

– Total loss of load and/or turbine trip,
– Loss of main heat sink (condenser),
– Inadvertent closure of a MSIV,
– SGTR,
– RCP seizure (locked rotor) or RCP shaft break, and
– Feedwater system piping failure.

Four divisions of the MSRIV Opening - Manual Function are required to be OPERABLE in:

– MODES 1, 2, 3, and
– MODE 4 when the SGs are relied upon for heat removal.

There is no NTSP associated with this Function.

There are no permissives associated with this Function.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

7. Main Steam Relief Train Isolation

a. Main Steam Relief Train (MSRT) Isolation – Low SG Pressure (Affected SG)

The MSRIVs are opened during events in order to control pressure in the SGs. In order to prevent a stuck open Main Steam Relief Control Valve (MSRCV) from causing an RCS cooldown and a risk of return to critical conditions, the MSRIV and MSRCV both receive a closing order in the event of a low SG pressure condition.

This Function mitigates the following postulated accidents or AOOs:

– Excessive increase in secondary steam flow,
– SGTR,
– Loss of main heat sink (condenser),
– Inadvertent opening of SG safety or relief valve, and
– MSLB.

Four divisions of the MSRT Isolation - Low SG Pressure (Affected SG) Function are required to be OPERABLE in:

– MODES 1, 2, and
– MODE 3 with P12 permissive inhibited.

This Function utilizes the SG Pressure sensors.

The NTSP is low enough to avoid spurious operation and high enough to limit the rate of RCS cooldown.

Inhibition of the P12 permissive automatically enables the MSRT Isolation - Low SG Pressure Function when the pressure is greater than or equal to approximately 2005 psia. When below this threshold, the Function is disabled by manual validation of the P12 permissive.

b. MSRT Isolation – Manual

The capability for manual system-level isolation of the MSRT on a per train basis is provided on the SICS in the MCR. Two manual system-level isolation controls are provided per MSRT. Any one of these two controls isolates the desired MSRT.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

This Function mitigates the following postulated accidents or AOOs:

– Excessive increase in secondary steam flow,
– SGTR,
– Loss of main heat sink (condenser),
– Inadvertent opening of SG safety or relief valve, and
– MSLB.

Four divisions of the MSRT Isolation - Manual Function are required to be OPERABLE in:

– MODES 1, 2, and
– MODE 3 with P12 permissive inhibited.

There is no NTSP associated with this Function.

Inhibition of the P12 permissive automatically enables the MSRT Isolation - Manual Function when the pressure is greater than or equal to approximately 2005 psia. When below this threshold, the Function is disabled by manual validation of the P12 permissive.

8. Main Steam Isolation

a. Main Steam Isolation - High SG Pressure Drop (All SGs)

In case of a secondary side steam line or feedwater system pipe break, the affected SG depressurizes. This Function isolates all four SGs in order to:

– Prevent draining of unaffected SG,
– Limit return to criticality conditions due to a overcooling transient,
– Limit the release of radioactivity, and
– Limit mass and energy releases into the containment.

This Function mitigates the following postulated accidents or AOOs:

– Excessive increase in secondary steam flow,
– Spurious opening of one SG safety or relief valve,
– Steam system piping failure, and
– Feedwater system piping failure.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

Four divisions of the Main Steam Isolation - High SG Pressure Drop (All SGs) Function are required to be OPERABLE in MODES 1 and 2, and in MODE 3 when all MSIVs are closed and deactivated.

This Function utilizes the SG Pressure sensors.

The NTSP is low enough to avoid SG pressure fluctuations during normal operation and high enough to isolate an SG and limit the blowdown to the value assumed in the safety analysis.

The condition to be detected is an SG pressure drop greater than a specified value. This is accomplished by using a variable pressure setpoint tracking the steam line pressure with a constant offset. The setpoint has a limitation on its maximum pressure and its maximum rate of decrease. If the steam line pressure increases, the setpoint will increase until the limitation on maximum pressure is reached. The maximum value of the setpoint is limited in order to avoid Main Steam isolation during an SG pressure decrease following a reactor trip and turbine trip, which would result in an SG overpressure condition. If the steam line pressure decreases, the setpoint will follow the decrease as long as the rate is less than or equal to the limitation on maximum rate of decrease. If the steam line pressure decreases more rapidly than the limitation on the maximum rate of decrease, the margin between the actual pressure and the setpoint will decrease until the steam line pressure equals the setpoint and protective action occurs.

There are no permissives associated with this Function.

b. Main Steam Isolation - Low SG Pressure (All SGs)

For most main steam line or feedwater pipe breaks, the affected SG depressurizes. For small breaks, the setpoint for Main Steam Isolation - High SG Pressure Drop may not be reached. This Function isolates all four SG on the main steam side in the event of a secondary side break in order to:

– Prevent draining of unaffected SGs,
– Limit the return to critical conditions due to a overcooling transient,
– Limit the release of radioactivity, and
– Limit mass and energy releases into the containment.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

This Function mitigates the following postulated accidents or AOOs:

– Excessive increase in secondary steam flow,
– Spurious opening of one SG safety or relief valve,
– Steam system piping failure, and
– Feedwater system piping failure.

Four divisions of the Main Steam Isolation - Low SG Pressure (All SGs) Function are required to be OPERABLE in:

– MODES 1, 2, and
– MODE 3 with P12 permissive inhibited, except when all MSIVs are closed and deactivated.

This Function utilizes the SG Pressure sensors.

The NTSP is low enough to avoid SG pressure fluctuations during normal operation and high enough to isolate an SG and limit the blowdown to the value assumed in the safety analysis.

Inhibition of the P12 permissive automatically enables the Main Steam Isolation - Low SG Pressure (All SGs) Function when the pressurizer pressure is greater than or equal to approximately 2005 psia. When below this threshold, the Function is disabled by manual validation of the P12 permissive.

c. Main Steam Isolation - High Containment Pressure (All SGs)

For most main steam line pipe breaks, the affected SG depressurizes. For small breaks, the setpoint for Main Steam Isolation - SG Pressure Drop or Low SG Pressure may not promptly detect the break. This Function isolates all four main steam lines in the event of a small steam line break in order to limit mass and energy releases into the containment.

This Function mitigates the following postulated accidents or AOOs:

– LOCA,
– Steam system piping failure, and
– Feedwater system piping failure.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

Four divisions of the Main Steam Isolation - High Containment Pressure (All SGs) function are required to be OPERABLE in MODES 1, 2, 3, and 4.

This Function utilizes the Containment Equipment Compartment Pressure and Containment Service Compartment Pressure (Narrow Range) sensors.

The NTSP is high enough to allow for small pressure increases in containment expected during normal operation (i.e., plant heatup) and is not indicative of an abnormal condition. It is low enough to initiate a main steam isolation when an abnormal condition is indicated.

There are no permissives associated with this function.

d. Main Steam Isolation - Manual

The capability for manual system-level actuation of main steam isolation is provided on the SICS in the MCR. This manual system-level initiation isolates the main steam trains. Four manual system-level initiation controls are provided, any two of which will actuate the main steam isolation.

This Function mitigates the following postulated accidents or AOOs:

– LOCA,
– Excessive increase in secondary steam flow,
– Spurious opening of one SG safety or relief valve,
– Steam system piping failure, and
– Feedwater system piping failure.

Four divisions of the Main Steam Isolation - Manual Function are required to be OPERABLE in MODES 1, 2, 3, and 4.

There is no NTSP associated with this Function.

There are no permissives associated with this Function.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

9. Main Feedwater Full Load Isolation

a. Main Feedwater Full Load Isolation – Reactor Trip Initiation (All SGs)

After a reactor trip initiation signal, a Main Feedwater (MFW) full load isolation is required. This avoids a mismatch between primary and secondary power. Such a mismatch could result in an RCS cooldown transient, with a potential inadvertent return to critical conditions.

Four divisions of the MFW Full Load Isolation - Reactor Trip Initiation (All SGs) Function are required to be OPERABLE in:

– MODES 1, 2, and
– MODE 3, except when all MFW Full Load isolation valves are closed and deactivated.

The sensors and NTSPs associated with this Function are described in LCO 3.3.1, “Reactor Trip Instrumentation,” for each individual automatic reactor trip Function.

There are no permissives associated with this Function.

b. Main Feedwater Full Load Isolation – High SG Level (Affected SGs)

In the case of an increasing SG level event, the MFW supply to the affected SG is isolated in order to avoid filling the SG, and subsequently introducing water into main steam line and MSRT. This function mitigates an increase in heat removal from the secondary system

This Function mitigates a feedwater flow increase.

Four divisions of the MFW Full Load Isolation - High SG Level (Affected SG) Function are required to be OPERABLE in:

– MODES 1, 2, 3, and
– MODE 4 with P13 permissive inhibited, except when all MFW Full Load isolation valves are closed and deactivated.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

This Function utilizes the SG Level (Narrow Range) sensors.

The MFW Full Load Isolation - High SG Level NTSP is high enough to avoid spurious actuation but low enough in order to prevent water level in the SG from rising and entering the steam line.

Inhibition of the P13 permissive automatically enables the MFW Full Load Isolation - High SG Level Function when the hot leg temperature is greater than or equal to approximately 200°F. When below this threshold, the Function is disabled by manual validation of the P13 permissive.

c. Main Feedwater Full Load Isolation – Manual

The capability for manual system-level isolation of MFW on a per-train basis is provided on the SICS in the MCR. This manual system-level initiation isolates both full load and SSS lines on the desired SG. Two manual system-level isolation controls are provided per MFW train. Either of the two controls isolates the MFW train.

This Function mitigates any event resulting in a reactor trip or a feedwater flow increase.

Four divisions of the MFW Full Load Isolation - High SG Level (Affected SG) Function are required to be OPERABLE in:

– MODES 1, 2, 3, and
– MODE 4, except when all MFW Full Load isolation valves are closed and deactivated.

There is no NTSP associated with this Function.

There are no permissives associated with this Function.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

10. Startup and Shutdown System (SSS) Isolation

a. SSS Isolation – High SG Pressure Drop (Affected SGs)

The affected SG depressurizes for excessive increase in secondary steam flow, steam system piping failure, and feedwater system piping failure. Also, the SSS isolation and control valves close in the affected SG.

A complete feedwater system isolation in the affected SG limits the coolant provided into the affected SG by the MFW/SSS. This action minimizes the mass and energy released into the containment and RCS cooldown. This function mitigates the following postulated accidents or AOOs:

– Excessive increase in secondary steam flow,
– Steam system piping failure,
– Spurious opening of one SG safety or relief valve, and
– Feedwater system piping failure.

Four divisions of the SSS Isolation - High SG Pressure Drop (Affected SG) Function are required to be OPERABLE in:

– MODES 1, 2, and
– MODE 3, except when all MFW Full Load and SSS isolation valves are closed and deactivated.

This function utilizes the SG Pressure sensors.

The NTSP is low enough to preclude spurious operation but high enough to terminate feedwater flow before overcooling of the primary system or depletion of secondary inventory.

The condition to be detected is an SG pressure drop greater than a specified value. This is accomplished by using a variable pressure setpoint tracking the steam line pressure with a constant offset. The setpoint has a limitation on its maximum pressure and its maximum rate of decrease. If the steam line pressure increases, the setpoint will increase until the limitation on maximum pressure is reached. If the steam line pressure decreases, the setpoint will follow the decrease as long as the rate is less than or equal to the limitation on maximum rate of decrease. If the steam line pressure decreases more rapidly than the limitation on the maximum rate of decrease, the margin between the actual pressure and the setpoint will decrease until the steam line pressure equals the setpoint and protective action occurs.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

There are no permissives associated with this function.

b. SSS Isolation – Low SG Pressure (Affected SGs)

The affected SG depressurizes in the event of a steam line or feedwater pipe failure. In the event of a small secondary side break for which the SG Pressure Drop signal is never reached, this function also isolates the SSS supply to the affected SG. This action minimizes the mass and energy released into the containment.

This function mitigates the following postulated accidents or AOOs:

– Excessive increase in secondary steam flow,
– Steam system piping failure,
– Spurious opening of one SG safety or relief valve, and
– Feedwater system piping failure.

Four divisions of the SSS Isolation - Low SG Pressure (Affected SG) Function are required to be OPERABLE in:

– MODES 1, 2, and
– MODE 3 with P12 permissive inhibited, except when all MFW Full Load and SSS isolation valves are closed and deactivated.

This Function utilizes the SG Pressure sensors.

The NTSP is low enough to preclude spurious operation but high enough to terminate feedwater flow before overcooling of the primary system or depletion of secondary inventory.

Inhibition of the P12 permissive automatically enables the SSS Isolation - Low SG Pressure (Affected SGs) Function when the pressurizer pressure is greater than or equal to approximately 2005 psia. When below this threshold, the function is disabled by manual validation of the P12 permissive.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

c. SSS Isolation – High SG Level for Period of Time (Affected SGs)

During an increase in SG level after a reactor trip, the SSS systems are isolated in the affected SG in order to avoid the SG filling up and thus carryover of water into main steam line and subsequent water discharge by MSRT.

This function mitigates the following postulated accidents or AOOs:

– Feedwater flow increase, and
– SGTR.

Four divisions of the SSS Isolation - High SG Level for Period of Time (Affected SG) Function are required to be OPERABLE in:

– MODES 1, 2, 3, and
– MODE 4 with P13 permissive inhibited, except when all MFW Full Load and SSS isolation valves are closed and deactivated.

This Function utilizes the SG Level (Narrow Range) sensors.

The NTSP is high enough to avoid spurious actuation but low enough in order to prevent water level in the SGs from rising and entering the steam lines.

Inhibition of the P13 permissive automatically enables the SSS Isolation on High SG Level for Period of Time function when the hot leg temperature is greater than or equal to approximately 200°F. When below this threshold, the function is disabled by manual validation of the P13 permissive.

d. SSS Isolation – High Containment Pressure (All SGs)

This Function isolates all four SSS lines in the event of a feedwater line break in order to limit mass and energy releases into the containment.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

This Function mitigates the following postulated accidents or AOOs:

– LOCA,
– Steam system piping failure, and
– Feedwater system piping failure.

Four divisions of the SSS Isolation - High Containment Pressure (All SGs) Function are required to be OPERABLE in MODES 1, 2, 3, and 4.

This Function utilizes the following sensors:

– Containment Equipment Compartment Pressure sensors, and
– Containment Service Compartment Pressure (Narrow Range) sensors,

The NTSP is high enough to allow for small pressure increases in containment expected during normal operation (i.e., plant heatup). It is low enough to initiate an SSS isolation when an abnormal condition is indicated.

There are no Permissives associated with this function.

e. SSS Isolation – Manual

The capability for manual system-level isolation of MFW on a per-train basis is provided on the SICS in the MCR. This manual system-level initiation isolates both full load and SSS lines on the desired SG. Two manual system-level isolation controls are provided per MFW train. Either of the two controls isolates the MFW train.

This Function mitigates the following postulated accidents or AOOs:

– Any event resulting in a reactor trip,
– Excessive increase in secondary steam flow,
– Steam system piping failure,
– Spurious opening of one SG safety or relief valve,
– Feedwater system piping failure,
– Feedwater flow increase,
– SGTR, and
– LOCA.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

Four divisions of the SSS Isolation - Manual Function are required to be OPERABLE in MODES 1, 2, 3, and 4.

There is no NTSP associated with this Function.

There are no permissives associated with this Function.

11. PSRV Opening

a. PSRV Opening – High Hot Leg Pressure

The integrity of the reactor pressure vessel must be ensured under all plant conditions. At low coolant temperature, the cylindrical part of the vessel could fail by brittle fracture before the design pressure of the RCS is reached. Therefore the low-temperature overpressure protection (LTOP) is ensured by opening of the PSRVs.

This function mitigates a low temperature overpressure event.

Four divisions of the PSRV Opening – High Hot Leg Pressure Function are required to be OPERABLE in MODE 4 when MHSI Large Miniflow Valves and PSRV OPERABILITY are required by LCO 3.4.11, "Low Temperature Overpressure Protection (LTOP)" and with P17 permissive validated.

Three divisions of the PSRV Opening – High Hot Leg Pressure Function are required to be OPERABLE in MODES 5 and 6 when MHSI Large Miniflow Valves and PSRV OPERABILITY are required by LCO 3.4.11, "Low Temperature Overpressure Protection (LTOP)" and with P17 permissive validated.

This function utilizes the Hot Leg Pressure (Narrow Range) sensors.

The NTSPs are high enough to prevent spurious operation but low enough to prevent RCS overpressurization.

Manual validation of the P17 permissive enables the PSRV Opening function when the cold leg temperature is less than the setpoint in the Pressure and Temperature Limits Report (approximately 248°F). When greater than or equal to this threshold, the function is automatically disabled by inhibition of the P17 permissive.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

b. PSRV Opening – Manual

The capability for manual system-level PSRV opening on a per-PSRV basis is provided to the operator on the SICS in the MCR. Two manual system-level initiation controls are provided per PSRV, both of which must be activated to open a PSRV.

Four divisions of the PSRV Opening – Manual Function are required to be OPERABLE in MODE 4 when MHSI Large Miniflow Valves and PSRV OPERABILITY are required by LCO 3.4.11, "Low Temperature Overpressure Protection (LTOP)."

Three divisions of the PSRV Opening – Manual Function are required to be OPERABLE in MODES 5 and 6 when MHSI Large Miniflow Valves and PSRV OPERABILITY are required by LCO 3.4.11, "Low Temperature Overpressure Protection (LTOP)."

There is no NTSP associated with this Function.

There are no permissives associated with this Function

12. SG Isolation

a. SG Isolation - Manual

The capability for manual system-level initiation of SG isolation on a per SG basis is provided on the SICS in the MCR. Four manual system-level initiation controls are provided per SG, any two of which will isolate the desired SG.

For an SGTR event, the operator is credited to perform a manual system-level initiation of SG isolation from the SICS in the MCR.

Four divisions of the SG Isolation - Manual Function are required to be OPERABLE in:

– MODES 1 and 2, and
– MODE 3 with P13 permissive inhibited.

There is no NTSP associated with this Function.

Inhibition of the P13 permissive automatically enables the SG Isolation – Manual Function when the hot leg temperature is greater than or equal to approximately 200°F. When below this threshold, the Function is disabled by manual validation of the P13 permissive.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

The manual system-level initiation satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

13. Turbine Trip on Reactor Trip Initiation

a. Turbine Trip on Reactor Trip Initiation - Automatic

A turbine trip is required following any reactor trip in order to avoid a mismatch between primary and secondary power, which would result in excessive RCS cooldown with a potential inadvertent return to critical conditions and power excursion.

The required divisions, sensors, NTSPs, and permissives for the Turbine Trip on Reactor Trip Initiation – Automatic Function are described in the Bases for LCO 3.3.1, “Reactor Trip Instrumentation.”

The Turbine Trip on Reactor Trip Initiation – Automatic Function is required to be OPERABLE in MODES 1 and 2.

b. Turbine Trip on Reactor Trip Initiation - Manual

The capability for manual system-level initiation of a turbine trip is provided on the SICS in the MCR. Four manual system-level initiation controls are provided; the activation of any two of the four results in turbine trip.

Four divisions of the Turbine Trip on Reactor Trip Initiation - Manual Function are required to be OPERABLE in MODES 1 and 2.

There is no NTSP associated with this Function.

There are no permissives associated with this Function.

14. Hydrogen Mixing Dampers Opening

a. Hydrogen Mixing Dampers Opening – High Containment Pressure

In case of a postulated initiating event leading to water or steam discharge into the containment, internal containment dampers are opened in order to promote containment atmospheric mixing.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

This Function mitigates the following postulated accidents or AOOs:

– Rod ejection,
– LOCA,
– MSLB inside containment, and
– Feedwater line break inside containment.

Four divisions of the automatic Hydrogen Mixing Dampers Opening - High Containment Pressure Function are required to be OPERABLE in MODES 1, 2, 3, and 4.

This function utilizes the Containment Service Compartment Pressure (Narrow Range) sensors.

The NTSP is high enough to avoid spurious operation but low enough to ensure offsite dose consequences are maintained below 10 CFR 50.34 and 10 CFR 100.21 limits.

There are no permissives associated with this function.

b. Hydrogen Mixing Dampers Opening – High Containment Compartments Delta Pressure

In case of a postulated initiating event leading to water or steam discharge into the containment, internal containment dampers are opened in order to promote containment atmospheric mixing.

This Function mitigates the following postulated accidents or AOOs:

– Rod ejection,
– LOCA,
– MSLB inside containment, and
– Feedwater line break inside containment.

Four divisions of the automatic Hydrogen Mixing Dampers Opening - High Containment Compartments Delta Pressure Function are required to be OPERABLE in MODES 1, 2, 3, and 4.

This function utilizes the Containment Equipment Compartment / Containment Service, and Compartment Delta Pressure sensors.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

The NTSP is high enough to avoid spurious operation but low enough to ensure offsite dose consequences are maintained below 10 CFR 50.34 and 10 CFR 100.21 limits.

There are no permissives associated with this function.

c. Hydrogen Mixing Dampers Opening – Manual

The capability for manual system-level initiation of this function is provided on the SICS in the MCR. Four manual system-level initiation controls are provided, any two of which will open the Hydrogen Mixing Dampers.

Four divisions of the Hydrogen Mixing Dampers Opening - Manual Function are required to be OPERABLE in MODES 1, 2, 3, and 4.

There is no NTSP associated with this Function.

There are no permissives associated with this Function.

15. Steam Generator Blowdown Cross-Tie Valve Opening

a. Steam Generator Blowdown Cross-Tie Valve Opening - Manual

The capability for component-level control of the blowdown valves is available to the operator on the SICS in the MCR. One switch is provided per valve. For small main steam line breaks (MSLB) and FWLB, manual initiation from the SICS is credited with closing the blowdown valves.

This Function mitigates the following postulated accidents or AOOs:

– Feedwater system piping failure,
– Loss of Normal Feedwater, and
– LOOP.

Four divisions of the Steam Generator Blowdown Cross-Tie Valve Opening - Manual Function are required to be OPERABLE in:

– MODES 1, 2, and
– MODE 3 with P18 permissive validated.

There is no NTSP associated with this Function.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

Validation of the P18 permissive automatically enables the Steam Generator Blowdown Cross-Tie Valve Opening - Manual Function when the Hot Leg Temperature (Wide Range) measurement is less than approximately 194°F. When the temperature is greater than or equal to this threshold, the Function is automatically disabled by inhibition of the P18 permissive.

The manual component-level initiation satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

16. SIS Hot Leg Injection Valve Opening

a. SIS Hot Leg Injection Valve Opening - Manual

The capability for component-level control of the blowdown valves is available to the operator on the SICS in the MCR. One switch is provided per valve.

The U.S. EPR provides the operator the capability to redirect an LHSI train so that at least 75 percent of it is injected through the hot leg letdown line of the residual heat removal system (RHRS). Analyses show that switching the Low Head Safety Injection to hot leg injection is effective at limiting the boron concentration in the core region regardless of the break location.

Four divisions of the SIS Hot Leg Injection Valve Opening - Manual Function are required to be OPERABLE in:

– MODES 1 and, 2,
– MODE 3 with P16 permissive validated, and
– MODE 4.

There is no NTSP associated with this Function.

There are no permissives associated with this Function.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

17. MHSI Large Miniflow Valves

a. MHSI Large Miniflow Valves - Interlock

The MHSI pumps are used to inject borated water from the in-containment refueling water storage tank (IRWST) into the cold legs when a safety injection signal is present. A large miniflow line branches off from the discharge side of each MHSI pump and provides a path, through a motor operated isolation valve, to the IRWST. These isolation valves are interlocked in the open position during low temperature operations to reduce the MHSI injection pressure. The interlock holding open the MHSI large miniflow valves protects against brittle fracture of the reactor pressure vessel and protects the RHR system from over-pressurization when it is connected to the RCS.

Four divisions of the MHSI Large Miniflow Valves - Interlock Function are required to be OPERABLE in MODE 4 with P17 permissive validated and when the MHSI Large Miniflow Valves and PSRV OPERABILITY are required by LCO 3.4.11, “Low Temperature Overpressure Protection (LTOP).”

Two divisions of the MHSI Large Miniflow Valves - Interlock Function are required to be OPERABLE in MODES 5 and 6 with P17 permissive validated and when the MHSI Large Miniflow Valves and PSRV OPERABILITY are required by LCO 3.4.11, “Low Temperature Overpressure Protection (LTOP).”

Below the P17 permissive temperature threshold, the large miniflow line isolation valves are interlocked in the open position to make brittle fracture protection via the PSRVs effective. When the P14 permissive is validated and one or more trains of RHR are connected to the RCS, the MHSI large miniflow valves are interlocked in the open position to provide overpressure protection of the RHR system.

Sensors for each of the permissive are identified in the Bases for LCO 3.3.3, “Permissive Instrumentation.”

b. MHSI Large Miniflow Valves - Manual

The capability for component-level control of the MHSI Large Miniflow valves is available to the operator on the SICS in the MCR. One switch is provided per valve.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

Four divisions of the MHSI Large Miniflow Valves - Manual Function are required to be OPERABLE in MODE 4 when the MHSI Large Miniflow Valves and PSRV OPERABILITY are required by LCO 3.4.11, “Low Temperature Overpressure Protection (LTOP).”

Two divisions of the MHSI Large Miniflow Valves - Manual Function are required to be OPERABLE in MODES 5 and 6 when the MHSI Large Miniflow Valves and PSRV OPERABILITY are required by LCO 3.4.11, “Low Temperature Overpressure Protection (LTOP).”

There are no permissives associated with this Function.

18. Extra Borating System (EBS) Actuation

a. EBS Actuation - Manual

The capability for manual system-level initiation of the EBS is provided on the SICS in the MCR. There are two manual Extra Borating System Actuation switches in Divisions 1 and 4 only (four switches total).

These switches are used to mitigate a SGTR and for cooldown from other design basis events.

Two divisions of the EBS Actuation switches (Division 1 and Division 4) are required to be OPERABLE in MODES 1, 2, 3, 4, and 5.

There are no permissives associated with this Function.

The manual system-level initiation satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

b. EBS Isolation - Manual

The capability for manual system-level initiation of the EBS is provided on the SICS in the MCR. There are two manual EBS Isolation switches in Divisions 1 and 4 only (four switches total).

These switches are used to mitigate a EBS malfunction event.

Two divisions of the EBS Isolation switches (Division 1 and Division 4) are required to be OPERABLE in MODES 1, 2, 3, 4, and 5.

There are no permissives associated with this Function.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

The manual system-level initiation satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

19. Operational I&C Disable Switch

a. Operational I&C Disable Switch - Manual

The SICS manual component level commands are momentary signals that are removed once the actuator has reached its final limit position. Once the SICS component level command signal is removed, the Process Automation System (PAS) has the ability to manipulate the actuator. This may be undesirable to the operator controlling the device. Therefore, four safety-related Operational I&C Disable switches are implemented to prevent PAS from manipulating the actuator.

Four divisions of the Operational I&C Disable Switch - Manual switches are required to be OPERABLE in MODES 1, 2, 3, and 4. Three divisions of the Operational I&C Disable Switch - Manual switches are required to be OPERABLE in MODES 5 and 6 and during the movement of irradiated fuel assemblies.

There is no NTSP associated with this Function.

There are no permissives associated with this Function.

20. Actuation Logic

Four divisions of the Actuation Logic are required to be OPERABLE in MODES 1, 2, 3, and 4. Three divisions of the Actuation Logic are required to be OPERABLE in MODES 5 and 6 and during the movement of irradiated fuel assemblies.

This Function does not utilize any sensors.

There is no NTSP associated with this Function.

There are no permissives associated with this Function.

ACTIONS

The most common causes of division inoperability are outright failure or drift of the sensor sufficient to exceed the tolerance allowed by the plant specific setpoint analysis. Typically, the drift is found to be small and results in a delay of actuation rather than a total loss of function. This determination is generally made during the performance of a

BASES

ACTIONS (continued)

CALIBRATION when the sensor is set up for adjustment to bring it to within specification. If an as-found sensor calibration setting value is non-conservative with respect to the Allowable Value, the sensor is immediately declared inoperable, and the appropriate Condition(s) must be entered.

In the event that any sensor or function processor is found inoperable, then all affected Trip/ESF/Permissive Functions provided by that sensor or function processor must be declared inoperable, and the plant must enter any applicable Condition for the particular Trip/ESF/Permissive Function affected.

When the number of inoperable Functions exceeds that specified in Table 3.3.2-1, redundancy is lost and actions must be taken to restore the required redundancy.

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

A.1

Condition A applies to all ESFAS Instrumentation Functions. Condition A addresses the situation where one or more Functions with one or more divisions are inoperable. The Required Action is to refer to Table 3.3.2-1 and to take the Required Actions for the Functions affected. The Completion Times are those from the referenced Conditions and Required Actions.

B.1

Condition B applies when one Input & Acquisition Logic division is inoperable. In this condition, the minimum number of OPERABLE divisions to read the plant parameter, perform conditioning, calculations, compare the values to setpoints, and sending to the voting logic during an AOO or postulated accident coupled with a single failure is still available. Verification that the Actuation Logic voting has been modified ensures the Protection System reflects the condition. The Completion Time of 6 hours is reasonable considering the availability of automatic actuation and the low probability of an AOO or postulated accident occurring during this time.

BASES

ACTIONS (continued)

C.1 and C.2

Condition C applies when one Input & Acquisition Logic division is inoperable. In this condition, the minimum number of OPERABLE divisions to read the plant parameter, perform conditioning, calculations, compare the values to setpoints, and sending to the voting logic during an AOO or postulated accident coupled is still available. Verification that the Actuation Logic voting has been modified ensures the Protection System reflects the condition. The Completion Time of 6 hours is reasonable considering the availability of automatic actuation and the low probability of an AOO or postulated accident occurring during this time. The Completion Time of 72 hours is reasonable considering that there are two divisions available, the low probability of an event occurring during this interval, and the time necessary for repairs.

D.1, D.2, and D.3

Condition D applies when two Input & Acquisition Logic divisions are inoperable. In this condition, the minimum number of OPERABLE divisions to read the plant parameter, perform conditioning, calculations, compare the values to setpoints, and sending to the voting logic during an AOO or postulated accident is still available.

A Note states that Required Action D.1 is only applicable if two Input & Acquisition Logic divisions which support the Main Steam Relief Isolation Valve Opening – High SG Pressure (Affected SG) Function are inoperable. If the two Input & Acquisition Logic divisions which support the Main Steam Relief Isolation Valve Opening – High SG Pressure (Affected SG) Function are not restored to OPERABLE status within the required Completion Time; the plant must be placed in a least MODE 1 with THERMAL POWER to < 50% RTP within 4 hours so that the available Main Steam Safety Valves relieving capacity meets ASME Code, Section III requirements for the power level.. The Completion Time of 4 hours is reasonable to reach MODE 1 with THERMAL POWER < 50% RTP from full power operation in an orderly manner and without challenging plant systems.

For all ESFAS Instrumentation Functions with two Input & Acquisition Logic divisions inoperable, verification that the Actuation Logic voting has been modified ensures the configuration of the Protection System logic reflects the plant condition. The Completion Time of 6 hours is

BASES

ACTIONS (continued)

reasonable considering the availability of automatic actuation and the low probability of an AOO or postulated accident occurring during this time. The Completion Time of 72 hours is reasonable considering that there are two OPERABLE Input & Acquisition Logic divisions, the low probability of an event occurring during this interval, and the time necessary for repairs.

E.1 and E.2

Condition E applies when one required Manual division is inoperable. In this condition, the remaining OPERABLE Manual divisions are available to send a trip signal during an AOO or postulated accident coupled with a single failure.

The OPERABILITY of the other Manual divisions must be verified within 6 hours. The Completion Time of 6 hours is reasonable considering that there are two Manual divisions available and the low probability of an event occurring during this interval. One inoperable Manual division must be restored to OPERABLE status within 72 hours. The Completion Time of 72 hours is reasonable considering that there are two Manual divisions available, the low probability of an event occurring during this interval, and the time necessary for performing the repairs.

F.1

Condition F applies when one required Manual division is inoperable. In this condition, the remaining OPERABLE Manual divisions are available to send a trip signal during an AOO or postulated accident coupled with a single failure.

The OPERABILITY of the other Manual divisions must be verified within 6 hours. The Completion Time of 6 hours is reasonable considering that there are three Manual divisions available and the low probability of an event occurring during this interval.

G.1

Condition G applies when one required Manual division is inoperable. The Required Action is to immediately enter the applicable Conditions and Required Actions of LCO 3.7.4, "Main Steam Relief Trains (MSRT)" for valve(s) made inoperable by the ESFAS Instrumentation. The purpose of each referenced action is addressed in the Bases for this section. The Completion Time of immediately is consistent with the required times for actions requiring prompt attention.

BASES

ACTIONS (continued)

H.1 and H.2

Condition H applies when two Manual division are inoperable. In this condition, the remaining OPERABLE Manual divisions are available to send a trip signal during an AOO or postulated accident.

The OPERABILITY of the other Manual divisions must be verified within 6 hours. The Completion Time of 6 hours is reasonable considering that there are two Manual divisions available and the low probability of an event occurring during this interval. One inoperable Manual division must be restored to OPERABLE status within 72 hours. The Completion Time of 72 hours is reasonable considering that there are two Manual divisions available, the low probability of an event occurring during this interval, and the time necessary for performing the repairs.

I.1 and I.2

Condition I applies when one Manual division is inoperable. In this condition, the remaining OPERABLE Manual divisions are available to send a trip signal during an AOO or postulated accident coupled with a single failure.

The OPERABILITY of the other Manual divisions must be verified within 6 hours. The Completion Time of 6 hours is reasonable considering that there are two Manual divisions available and the low probability of an event occurring during this interval. One inoperable Manual division must be restored to OPERABLE status within 72 hours. The Completion Time of 72 hours is reasonable considering that there are two Manual divisions available, the low probability of an event occurring during this interval, and the time necessary for performing the repairs.

J.1 and J.2

Condition J addresses the inability to complete the remedial measures in the time allowed by Required Actions I.1. The plant must be brought to a MODE where the LCO is no longer applicable. To achieve this status, the plant must be brought to at least MODE 4 without reliance upon steam generator for heat removal. The Completion Times of 6 hours to reach MODE 3 and 24 hours to reach MODE 4 without reliance upon steam generator for heat removal are reasonable, based on operating experience, to reach the required unit conditions from full power conditions in an orderly manner and without challenging plant systems

BASES

ACTIONS (continued)

K.1 and K.2

Condition K applies when one required SIS Actuation – Low Hot Leg Loop Level Function Input & Acquisition Logic division is inoperable. In this condition, the automatic mitigation of events in MODES 5 and 6 that could result in a decrease in RCS inventory may have been impacted. Operations that could reduce RCS inventory shall be immediately suspended. Actions to restore the required division to OPERABLE status must also be initiated immediately. The Completion Time of immediately is consistent with the required times for actions requiring prompt attention.

L.1

Condition L addresses the failure of two or more required Input & Acquisition Logic divisions, two or more required Manual divisions, or the inability to complete the remedial measures in the time allowed by Required Actions C.1, C.2, E.1, or E.2. In this condition, the automatic or manual mitigation of low temperature overpressure events may have been impacted. The applicable Conditions and Required Actions of LCO 3.4.11, “Low Temperature Overpressure Protection (LTOP),” are required to be entered for PSRV(s) or MHSI Large Miniflow Valve(s) made inoperable by ESFAS instrumentation. The actions of LCO 3.4.11, "Low Temperature Overpressure Protection (LTOP)," provide adequate compensatory actions to assure plant safety. The Completion Time of immediately is consistent with the required times for actions requiring prompt attention.

M.1 and M.2

Condition M addresses the failure of two or more required Input & Acquisition Logic divisions, two or more required Manual divisions, or the inability to complete the remedial measures in the time allowed by Required Actions C.1, C.2, E.1, or E.2. In this condition, the automatic or manual SIS Actuation – Low Hot Leg Loop Level Function Input & Acquisition Logic division is inoperable. The mitigation of events in MODES 5 and 6 that could result in a decrease in RCS inventory may have been impacted. Operations that could reduce RCS inventory shall be immediately suspended. Actions to restore the required division to OPERABLE status must also be initiated immediately. The Completion Time of immediately is consistent with the required times for actions requiring prompt attention.

BASES

ACTIONS (continued)

N.1

Condition N addresses the failure of three or more Input & Acquisition Logic divisions, two or more Manual divisions, or the inability to complete the remedial measures in the time allowed by Required Actions B.1, D.1, D.2, D.3, I.1, or I.2. In this condition, the automatic or manual mitigation of low temperature overpressure events may have been impacted. The applicable Conditions and Required Actions of LCO 3.4.11, “Low Temperature Overpressure Protection (LTOP),” are required to be entered for PSRV(s) or MHSI Large Miniflow Valve(s) made inoperable by ESFAS instrumentation. The actions of LCO 3.4.11, "Low Temperature Overpressure Protection (LTOP)," provide adequate compensatory actions to assure plant safety. The Completion Time of immediately is consistent with the required times for actions requiring prompt attention.

O.1

Condition O addresses the failure of three or more Input & Acquisition Logic divisions, three or more Manual divisions, or the inability to complete the remedial measures in the time allowed by Required Actions B.1, D.1, D.2, or D.3. In this condition, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 with P12 validated (Pressurizer Pressure Lower than Setpoint) within 6 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.

P.1

Condition P addresses the failure of three or more Input & Acquisition Logic divisions or the inability to complete the remedial measures in the time allowed by Required Actions B.1, D.1, D.2, or D.3. In this condition, the SIS Actuation – Low Delta P_{sat} Function Input & Acquisition Logic division is inoperable. The plant must be brought to a MODE where the LCO is no longer applicable. The Completion Time of 12 hours to reach MODE 4 with P15 validated 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

ACTIONS (continued)

Q.1 and Q.2

Condition Q addresses the failure of three or more Input & Acquisition Logic divisions, three or more Manual divisions, or the inability to complete the remedial measures in the time allowed by Required Actions B.1, D.1, D.2, or D.3. In this condition, the associated Functions are inoperable and the plant must be brought to a MODE where the associated LCO is no longer applicable. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and MODE 4 within 12 hours. The Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

R.1 and R.2

Condition R addresses the failure of three or more Input & Acquisition Logic divisions, three or more Manual divisions, or the inability to complete the remedial measures in the time allowed by Required Actions B.1, D.1, D.2, or D.3. In this condition, the associated Functions are inoperable and the plant must be brought to a MODE where the associated LCO is no longer applicable. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and MODE 5 within 36 hours. The Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

S.1

Condition S addresses the failure of three or more Input & Acquisition Logic divisions, three or more Manual divisions, or the inability to complete the remedial measures in the time allowed by Required Actions B.1, D.1, D.2, or D.3. In this condition, the associated Functions are inoperable and the plant must be brought to a MODE where the associated LCO is no longer applicable. To achieve this status, the plant must be brought to at least MODE 3 with all main steam isolation valves closed and deactivated within 6 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.

BASES

ACTIONS (continued)

T.1

Condition T addresses the failure of three or more Input & Acquisition Logic divisions or the inability to complete the remedial measures in the time allowed by Required Actions B.1, D.1, D.2, or D.3. In this condition, the Main Feedwater Full Load Isolation Functions are inoperable and the plant must be brought to a MODE where the associated LCO is no longer applicable. To achieve this status, the plant must be brought to at least MODE 3 with all main feedwater isolation valves closed and deactivated within 6 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.

U.1 and U.2

Condition U addresses the failure of three or more Input & Acquisition Logic divisions, three or more Manual divisions, or the inability to complete the remedial measures in the time allowed by Required Actions B.1, D.1, D.2, or D.3. In this condition, the associated Functions are inoperable and the plant must be brought to a MODE where the associated LCO is no longer applicable. To achieve this status, the plant must be brought to at least MODE 4 without reliance upon steam generator for heat removal. The Completion Times of 6 hours to reach MODE 3 and 24 hours to reach MODE 4 without reliance upon steam generator for heat removal 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.

V.1, V.2 and V.3

Condition V addresses the failure of three or more Manual divisions or the inability to complete the remedial measures in the time allowed by Required Actions F.1 or H.1. In this condition, the Extra Borating System Actuation – Manual Function is inoperable. Operations involving positive reactivity additions that could result in loss of required shutdown margin or boron concentration shall be immediately suspended. The Completion Time of immediately is consistent with the required times for actions requiring prompt attention.

BASES

ACTIONS (continued)

The plant must be brought to a MODE where the associated LCO is no longer applicable. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and MODE 5 within 36 hours. The Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

W.1. W.2, W.3, W.4.1, W.4.2, and W.5

Condition W addresses the failure of two or more required Manual divisions or the inability to complete the remedial measures in the time allowed by Required Action E.1. In this condition, the Operational I&C Disable Switch – Manual Function is inoperable. The following actions shall be taken immediately:

- Suspend operations involving positive reactivity additions that could result in loss of required SDM;
- Suspend activities that could reduce RCS inventory;
- Enter the applicable Conditions and Required Actions of LCO 3.4.11, “Low Temperature Overpressue Protection (LTOP),” for PSRV(s) or MHSI Large Miniflow Valve(s) made inoperable by the ESFAS instrumentation.
- Place both CREF trains in emergency mode;
- Suspend movement of irradiated fuel assemblies; and
- Initiate action to restore required division(s) to OPERABLE status.

The Completion Time of immediately is consistent with the required times for actions requiring prompt attention.

X.1 and X.2

Condition X addresses the failure of one or more required SIS Actuation – Manual division(s) or the inability to complete the remedial measures in the time allowed by Required Action H.1. In this condition, activities that could reduce RCS inventory must be immediately suspended and action immediately initiated to restore the required division(s) to OPERABLE status. The Completion Time of immediately is consistent with the required times for actions requiring prompt attention.

BASES

ACTIONS (continued)

Y.1

The Required Action is modified by a Note that clarifies its applicability. This Required Action is only applicable to the EFWS Actuation, Common SGBD Valve Isolation, Partial Cooldown Actuation, Turbine Trip on Reactor Trip Initiation, and Hydrogen Mixing Dampers Opening Functions.

Condition Y addresses the failure of one Actuation Logic division. In this condition, the minimum number of OPERABLE divisions to send the voting logic during an AOO or postulated accident coupled with a single failure is still available. The OPERABILITY of the other Actuation Logic division must be verified within 6 hours. The Completion Time of is reasonable considering the low probability of an event occurring during this interval and the time necessary for repairs.

Z.1

The Required Action is modified by a Note that clarifies its applicability. This Required Action is only applicable to the SIS Actuation, EFWS Isolation, MSRIV Opening, MSRT Isolation, Main Steam Isolation, Main Feedwater Full Load Isolation, SSS Isolation, SG Isolation, SGBT Cross-Tie Valve Opening, SIS Hot Leg Injection Valve Opening, and Extra Borating System Actuation Functions.

Condition Z addresses the failure of one Actuation Logic division. In this condition, the minimum number of OPERABLE divisions to send the voting logic during an AOO or postulated accident is still available. The OPERABILITY of the required Actuation Logic division must be restored within 72 hours. The Completion Time of 72 hours is reasonable considering the low probability of an event occurring during this interval and the time necessary for repairs.

AA.1

The Required Action is modified by a Note that clarifies its applicability. This Required Action is only applicable to the PSRV Opening and MHSI Large Miniflow Valves Functions.

BASES

ACTIONS (continued)

Condition AA addresses the failure of one or more Actuation Logic divisions. In this condition, the automatic or manual mitigation of low temperature overpressure events may have been impacted. The applicable Conditions and Required Actions of LCO 3.4.11, “Low Temperature Overpressure Protection (LTOP),” are required to be entered for PSRV(s) or MHSI Large Miniflow Valve(s) made inoperable by ESFAS instrumentation. The actions of LCO 3.4.11, "Low Temperature Overpressure Protection (LTOP)," provide adequate compensatory actions to assure plant safety. The Completion Time of immediately is consistent with the required times for actions requiring prompt attention.

BB.1

The Required Action is modified by a Note that clarifies its applicability. This Required Action is only applicable to the EFWS Actuation, Common SGBD Valve Isolation, Partial Cooldown Actuation, Turbine Trip on Reactor Trip Initiation, and Hydrogen Mixing Dampers Opening Functions.

Condition BB addresses the failure of two Actuation Logic divisions. In this condition, the minimum number of OPERABLE divisions to send the voting logic during an AOO or postulated accident is still available. The OPERABILITY of one Actuation Logic division must be restored within 72 hours. The Completion Time of 72 hours is reasonable considering the low probability of an event occurring during this interval and the time necessary for repairs.

CC.1, CC.2, CC.3.1, CC.3.2, CC.4.1, CC.4.2, CC.5, CC.6.1, CC.6.2, CC.7.1, CC.7.2, CC.8.1, CC.8.2, CC.9.1 and CC.9.2

Condition CC addresses the failure of two or more required Actuation Logic divisions or the inability to complete the remedial measures in the time allowed by Required Actions Y.1, Z.1, or BB.1. In this condition, the automatic or manual mitigation of an AOO or postulated accident may have been impacted.

Required Action CC.1 is modified by a Note that clarifies its applicability. Required Action CC.1 is only applicable to the SIS Actuation – Low Pressurizer Pressure and Turbine Trip on Reactor Trip Initiation Functions. In this condition, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be

BASES

ACTIONS (continued)

brought to at least MODE 3 with P12 validated (Pressurizer Pressure Lower than Setpoint) within 6 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.

Required Action CC.2 is modified by a Note that clarifies its applicability. Required Action CC.2 is only applicable to the SIS Actuation – Low Delta P_{sat} Function. In this condition, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 4 with P15 validated (Hot Leg Pressure and Hot Leg Temperature Lower than Setpoints and No RCP in Operation) 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.

Required Actions CC.3.1 and CC.3.2 are modified by a Note that clarifies its applicability. Required Actions CC.3.1 and CC.3.2 are only applicable to the SIS Actuation – Low Hot Leg Loop Level and SIS Actuation – Manual Functions. In this condition, the Required Action is to immediately suspend activities that could reduce RCS inventory and initiated to restore the required division(s) to OPERABLE status. The Completion Times of immediately are consistent with the required times for actions requiring prompt attention.

Required Actions CC.4.1 and CC.4.2 are modified by a Note that clarifies their applicability. Required Action CC.4.1 and CC.4.2 are only applicable to the Main Steam Isolation – High Containment Pressure (All SGs), Main Steam Isolation – Manual, SSS Isolation – High Containment Pressure (All SGs), Hydrogen Mixing Dampers Opening, and SIS Hot Leg Injection Valve Opening – Manual Functions. In this condition, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and MODE 5 within 36 hours. The Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems

Required Action CC.5 is modified by a Note that clarifies its applicability. Required Action CC.5 is only applicable to the Main Feedwater Full Load Isolation – Reactor Trip Initiation (All SGs) Function. In this condition, the plant must be brought to a MODE in which the LCO does not apply. To

BASES

ACTIONS (continued)

achieve this status, the plant must be brought to at least MODE 3 within 6 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.

Required Actions CC.6.1 and CC.6.2 are modified by a Note that clarifies their applicability. Required Action CC.6.1 and CC.6.2 are only applicable to the Main Steam Isolation – High SG Pressure Drop (All SGs) and Main Steam Isolation – Low SG Pressure (All SGs) Functions. In this condition, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 with all main steam isolation valves closed and deactivated within 6 hours and MODE 4 within 24 hours. The Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

Required Actions CC.7.1 and CC.7.2 are modified by a Note that clarifies their applicability. Required Action CC.7.1 and CC.7.2 are only applicable to the Main Feedwater Full Load Isolation Function. In this condition, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 with all main feedwater isolation valves closed and deactivated within 6 hours and MODE 4 within 24 hours. The Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

Required Actions CC.8.1 and CC.8.2 are modified by a Note that clarifies their applicability. Required Action CC.8.1 and CC.8.2 are only applicable to the EFWS Isolation, Main Steam Relief Isolation Valve Opening, SSS Isolation – High SG Pressure Drop (Affected SG), SSS Isolation – Low SG Pressure (Affected SG), and SSS Isolation – High SG Level for Period of Time (Affected SG) Functions. In this condition, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 4 without reliance upon a steam generator for heat removal within 24 hours. The Completion Times of 6 hours to reach MODE 3 and 24 hours to reach MODE 4 without reliance upon steam generator for heat removal 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.

Required Actions CC.9.1 and CC.9.2 are modified by a Note that clarifies their applicability. Required Action CC.9.1 and CC.9.2 are only applicable to the EFWS Actuation – Low-Low SG Level (Affected SG), EFWS

BASES

ACTIONS (continued)

Isolation – High SG Level (Affected SG), Partial Cooldown Actuation – Automatic on SIS Actuation, Partial Cooldown Actuation – Manual Reset, MSRT Isolation, SSS Isolation – High SG Pressure Drop (Affected SG), SSS Isolation – Low SG Pressure (Affected SG), and SG Isolation – Manual Functions. In this condition, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and MODE 4 within 24 hours. The Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

DD.1.1, DD.1.2, DD.2, DD.3.1 and DD.3.2

Condition DD addresses the failure of three or more Actuation Logic divisions or the inability to complete the remedial measures in the time allowed by Required Actions Y.1, Z.1, or BB.1. In this condition, the automatic or manual mitigation of an AOO or postulated accident may have been impacted. Required Actions DD.1.1 and DD.1.2 are modified by a Note that clarifies its applicability. This Required Actions are only applicable to the Main Steam Isolation – High Containment Pressure (All SGs) and Main Steam Isolation – Manual Functions. In this condition, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and MODE 5 within 36 hours. The Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

Required Action DD.2 is modified by a Note that clarifies its applicability. Required Action DD.2 is only applicable to the Turbine Trip on Reactor Trip Initiation Function. In this condition, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 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.

Required Actions DD.3.1 and DD.3.2 are modified by a Note that clarifies its applicability. This Required Actions are only applicable to the EFWS Actuation – Manual (Affected SG), Common SGBD Valve Isolation – Manual – (Affected SG), EFWS Isolation – Manual (Affected SG), Partial Cooldown Actuation – Manual, Main Steam Relief Isolation valve Opening – High SG Pressure (Affected SG), Main Steam Relief Isolation valve

BASES

ACTIONS (continued)

Opening – Manual, Main Feedwater Full Load Isolation – Manual, SSS Isolation – High SG Level for Period of Time (Affected SG), SSS Isolation – Manual, PSRV Opening – Manual, and SGBD Cross-Tie Valve Opening – Manual Functions. In this condition, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 4 without reliance upon a steam generator for heat removal. The Completion Times of 6 hours to reach MODE 3 and 24 hours to reach MODE 4 without reliance upon steam generator for heat removal 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.

EE.1

Condition EE addresses the failure of one of two required Manual divisions. In this condition, the remaining OPERABLE Manual division is available to send a EFWS actuation signal during an AOO or postulated accident. The inoperable Manual division must be restored to OPERABLE status within 72 hours. The Completion Time of 72 hours is reasonable considering that one Manual division is still available, the low probability of an event occurring during this interval, and the time necessary for repairs.

FF.1

Condition FF addresses the failure of both required Manual division. In this condition, the EFWS Actuation – Manual Function is inoperable and the plant must be brought to a MODE where the associated LCO is no longer applicable. To achieve this status, the plant must be brought to MODE 4 without reliance upon steam generator for heat removal. The Completion Time of 24 hours 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

The Surveillance Requirements (SR) for each Function are identified by the SRs column of Table 3.3.2-1 for that Function. Most Functions are subject to CHANNEL CHECK, ACTUATION DEVICE OPERATIONAL TEST, CALIBRATION, SENSOR OPERATIONAL TEST, EXTENDED SELF TESTS, and RESPONSE TIME testing.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The SRs are modified by a Note. The Note directs the reader to Table 3.3.2-1 to determine the correct SRs to perform for each Function.

SR 3.3.2.1

Performance of the CHANNEL CHECK ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the 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; therefore, it is key in verifying that the instrumentation continues to operate properly between each CALIBRATION.

Agreement criteria are determined by the plant staff, based on a combination of the channel instrument uncertainties, including isolation, indication, and readability. If a channel is outside the criteria, it may be an indication that the sensor or the signal processing equipment has drifted outside its limit. If the channels are within the criteria, it is an indication that the channels are OPERABLE.

The Frequency of 31 days is based on operating experience that demonstrates that channel failure is rare. The CHANNEL CHECK supplements less formal checks of channels during operational use of the displays associated with the LCO required channels.

SR 3.3.2.2

A SENSOR OPERATIONAL TEST (SOT) is performed every 24 months to ensure the devices will perform their intended function when needed. The test is performed in accordance with the Setpoint Control Program. A SOT shall be the injection of a simulated or actual signal into the division as close to the sensor as practicable to verify OPERABILITY of all devices in the division required for division OPERABILITY. The SOT shall include the verification of the accuracy and time constants of the analog input modules.

The SOT may be performed by means of any series of sequential, overlapping, or total steps.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.2.3

A CALIBRATION of each sensor every 24 months ensures that each instrument division is reading accurately and within tolerance. The test is performed in accordance with the Setpoint Control Program. A CALIBRATION shall be the adjustment, as necessary, of the sensor output such that it responds within the necessary range and accuracy to known values of the parameter that the division monitors. The CALIBRATION shall encompass all devices in the division required for sensor OPERABILITY.

The CALIBRATION includes provisions for the following:

1. Evaluation of sensor performance to verify that the sensor is functioning as required prior to returning the sensor to service if the as-found sensor calibration setting values are outside their predefined as-found tolerance for the specified calibration settings (e.g., 0, 25, 50, 75, and 100 percent), but conservative with respect to the Allowable Value, and

2. Declaring the sensor immediately inoperable if the sensor cannot be calibrated such that the as-left sensor calibration setting values are within the specified as-left tolerance around the specified calibration settings (e.g., 0, 25, 50, 75, and 100 percent), at the completion of the surveillance.

The CALIBRATION may be performed by means of any series of sequential, overlapping, or total steps.

SR 3.3.2.4

The features of continuous self-monitoring of the Protection System are described in Reference 2. Additional tests, which require the function processor to be inoperable are not normally performed during operation. These EXTENDED SELF TESTS are performed at start-up of a function processor each cycle. The startup sequence is as follows:

– Hardware basic test using the internal diagnosis monitor,
– Start-up self-test of the operating system, and
– Switch over to normal operation after approximately two minutes.

Additional information is provided in Section 2 of Reference 2.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.2.5

SR 3.3.2.5 is the performance of an ACTUATING DEVICE OPERATIONAL TEST (ADOT) every 24 months. The ADOT may be performed by means of any series of sequential, overlapping, or total steps.

SR 3.3.2.6

SR 3.3.2.6 verifies that the NTSPs have been properly loaded into the applicable APUs.

SR 3.3.2.7

This surveillance verifies that the individual division actuation response times are less than or equal to the maximum values assumed in the accident analysis. Response time testing acceptance criteria are included in a document controlled under 10 CFR 50.59. Individual component response times are not modeled in the analyses.

The analyses model the overall or total elapsed time, from the point at which the parameter exceeds the trip setpoint value at the sensor to the point at which the equipment reaches the required functional state (e.g., valves in full closed position).

For divisions that include dynamic transfer functions (e.g., lag, lead/lag, rate/lag, etc.), the response time test may be performed with the transfer function set to one, with the resulting measured response time compared to the appropriate FSAR response time. Alternately, the response time test can be performed with the time constants set to their nominal value, provided the required response time is analytically calculated assuming the time constants are set at their nominal values. The response time may be measured by a series of overlapping tests such that the entire response time is measured.

BASES

SURVEILLANCE REQUIREMENTS (continued)

----------REVIEWER'S NOTE----------
The following Bases apply to plants that have obtained NRC approval to utilize allocations for selected components based on NRC-approved U.S. EPR-applicable Topical Reports.

[Response time may be verified by actual response time tests in any series of sequential, overlapping or total division measurements, or by the summation of allocated sensor, signal processing and actuation logic response times with actual response time tests on the remainder of the division. Allocations for sensor response times may be obtained from: (1) historical records based on acceptable response time tests (hydraulic, noise, or power interrupt tests), (2) in place, onsite, or offsite (e.g., vendor) test measurements, or (3) utilizing vendor engineering specifications. NRC-approved U.S. EPR-applicable Topical Report provides the basis and methodology for using allocated sensor response times in the overall verification of the division response time for specific sensors identified in the report. Response time verification for other sensor types must be demonstrated by test.

NRC-approved U.S. EPR-applicable Topical Report (provide reference) provides the basis and methodology for using allocated signal processing and actuation logic response times in the overall verification of the DCS division response time.

The allocations for sensor, signal conditioning, and actuation logic response times must be verified prior to placing the component in operational service and re-verified following maintenance that may adversely affect response time. In general, electrical repair work does not impact response time provided the parts used for repair are of the same type and value. One example where response time could be affected is replacing the sensing assembly of a transmitter.]

As appropriate, each division’s response must be verified every 24 months on a STAGGERED TEST BASIS. Testing of the final actuation devices is included in the testing. Response times cannot be determined during plant operation because equipment operation is required to measure response times. Experience has shown that these components usually pass this surveillance when performed at the 24 month Frequency. Therefore, the Frequency was concluded to be acceptable from a reliability standpoint.

BASES

REFERENCES

1. FSAR Section 7.3

2. ANP-10315P, Revision 1, “U.S. EPR Protection System Surveillance Testing and Teleperm XS Self-Monitoring Technical Report,” June 2011.

B 3.3 INSTRUMENTATION

B 3.3.3 Permissive Instrumentation

BASES

BACKGROUND

Refer to B 3.3.1, “Reactor Trip Instrumentation,” for background information on the Distributed Control System. Refer to B 3.3.2, “Engineered Safety Feature Actuation System (ESFAS) Instrumentation,” for background information that is generically applicable to U.S. EPR systems that perform Engineered Safety Feature (ESF) functions.

The Permissive Instrumentation is unique in that does not actuate any plant equipment. Operating bypasses of specific reactor trip and ESF functions are permitted when plant conditions dictate that the function is not needed, or that the function would prevent proper plant operation. These bypasses are implemented in the form of permissive signals (P#) that are generated within the Protection System. The applicable permissive signals (if any) associated with each reactor trip and ESF Function are identified in the description of each function in the Bases for LCO 3.3.1, “Reactor Trip Instrumentation,” and LCO 3.3.2, “Engineered Safety Feature Actuation System (ESFAS) Instrumentation.” The logic used to generate the permissive signals is described in Sections 7.2 and 7.3.

Permissive setpoints allow bypass of reactor trips or ESF functions when they are not required by the Safety Analysis. These permissives ensure that the starting conditions are consistent with the safety analysis, before preventative or mitigating actions occur. The permissives are only one of multiple conservative starting assumptions for the accident analysis. Therefore, permissive setpoints are not considered to be SL-LSSS.

SAFETY ANALYSES, LCO, and APPLICABILITY

analyses, LCO, and applicability information that applies to reactor trip functions. Refer to B 3.3.2, “Engineered Safety Feature Actuation System (ESFAS) Instrumentation,” for applicable safety analyses, LCO, and applicability information that applies to ESF functions.

The Permissive Instrumentation performs the following Functions:

1. P2 Automatic Validation

a. P2 Automatic Validation – Power Range Flux Measurement Higher than First Setpoint

The P2 Automatic Validation – Power Range Flux Measurement Higher than First Setpoint Function is representative of Power

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

Range Detector (PRD) neutron flux measurements higher than a low-power setpoint value. The P2 setpoint value corresponds to the value below which transients do not lead to risk of DNB (approximately 10% rated thermal power (RTP)).

The P2 Automatic Validation – Power Range Flux Measurement Higher than First Setpoint Function is utilized in the following reactor trips:

– Reactor Trip 1: DNBR - Low,
– Reactor Trip 2: DNBR with High Quality - Low,
– Reactor Trip 3: DNBR with Imbalance or Rod Drop (1/4) - Low,
– Reactor Trip 4: DNBR with High Quality and (Imbalance or Rod Drop) (1/4) – Low,
– Reactor Trip 5: DNBR with Rod Drop (2/4) – Low,
– Reactor Trip 6: Linear Power Density - High,
– Reactor Trip 10: Reactor Coolant System (RCS) Flow Rate – Low in Two Loops,
– Reactor Trip 12: Reactor Coolant Pump (RCP) Speed – Low in Two Loops, and
– Reactor Trip 15: Pressurizer Pressure - Low.

Four divisions of the P2 Automatic Validation – Power Range Flux Measurement Higher than First Setpoint Function are required to be OPERABLE in MODE 1.

This Function utilizes the PRDs.

To generate the permissive, neutron flux measurements from the PRDs are compared to the setpoint (approximately 10% RTP). When at least two measurements are greater than the setpoint, the permissive is automatically validated.

2. P3 Automatic Validation

a. P3 Automatic Validation - Power Range Flux Measurement Higher than Second Setpoint

The P3 permissive is representative of PRD neutron flux measurements higher than an intermediate power setpoint value. The P3 setpoint value corresponds to the value below which loss of one reactor coolant pump does not lead to risk of departure from nucleate boiling (DNB) (approximately 70% RTP).

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

The P3 permissive is utilized in Reactor Trip 11: RCS Flow Rate – Low-Low in One Loop.

Four divisions of the P3 Automatic Validation - Power Range Flux Measurement Higher than Second Setpoint Function are required to be OPERABLE in MODE 1.

This Function utilizes the Power Range Detectors sensors.

To generate the permissive, neutron flux measurements from the PRDs are compared to the setpoint (approximately 70% RTP). When at least two measurements are greater than the setpoint, the permissive is automatically validated.

3. P5 Automatic Validation

a. P5 Automatic Validation - Intermediate Range Flux Measurement Higher than Setpoint

The P5 permissive is representative of Intermediate Range Detector (IRD) neutron flux measurements above a low-power setpoint value. The P5 setpoint value corresponds to the boundary between the operating ranges of the Source Range Detectors and IRDs (greater than approximately 10^{-5} % RTP as indicated on the IRDs).

The P5 permissive is utilized in the following reactor trips:

– Reactor Trip 8: Core Power Level - High, and
– Reactor Trip 9: Saturation Margin - Low.

Four divisions of the P5 Automatic Validation - Intermediate Range Flux Measurement Higher than Setpoint Function are required to be OPERABLE in MODE 2.

This Function utilizes the IRD sensors.

To generate the permissive, neutron flux measurements from the IRDs are compared to the setpoint (greater than approximately 10^{-5} % RTP). When at least two measurements are greater than the setpoint, the permissive is automatically validated.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

4. P6 Automatic Inhibition

a. P6 Automatic Inhibition - Thermal Core Power Lower than Setpoint

The P6 permissive is representative of core THERMAL POWER above a low-power setpoint value corresponding to the boundary between the operating ranges of the IRDs and the PRDs (approximately 10% RTP).

The P6 permissive is utilized in the following reactor trips:

– Reactor Trip 13: Neutron Flux - High (Intermediate Range), and
– Reactor Trip 14: Doubling Time - Low.

Four divisions of the P6 Automatic Inhibition - Thermal Core Power Lower than Setpoint Function are required to be OPERABLE in MODE 1.

This Function utilizes the following sensors:

– Cold Leg Temperature (Narrow Range),
– Hot Leg Pressure (Wide Range),
– Hot Leg Temperature (Narrow Range),

These sensors are used to calculate core THERMAL POWER. To generate the permissive, these calculated core thermal power levels are compared to the setpoint (approximately 10% RTP). When at least three calculated core thermal power levels are greater than the setpoint, the operator is prompted to manually validate the permissive. Otherwise, the permissive is inhibited.

5. P7 Automatic Validation

a. P7 Automatic Validation - No RCPs in Operation

The P7 Automatic Validation - No RCPs in Operation permissive defines when RCPs are no longer in operation.

The P7 Automatic Validation - No RCPs in Operation permissive is utilized in the Chemical and Volume Control System (CVCS) Isolation - Anti-Dilution Mitigation (ADM) at Shutdown with No RCP in Operation Function.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

Three divisions of the P7 Automatic Validation - No RCPs in Operation Function are required to be OPERABLE in MODE 5.

This Function utilizes the following sensors:

– RCP Breaker Position Indication sensors,
– RCP Bus Breaker Position Indication sensors, and
– RCP Speed sensors.

To generate the permissive, when at least two of the following conditions are true, a signal is generated for that pump:

– RCP Breaker open position,
– RCP Bus Breaker open position,
– First RCP Speed measurement less than or equal to a setpoint (approximately 90%), and
– Second RCP Speed measurement less than or equal to a setpoint (approximately 90%).

When signals are generated for all four pumps, a delay time (approximately 600 seconds) is started. After the delay time has expired, the permissive is automatically validated.

6. P7 Automatic Inhibition

a. P7 Automatic Inhibition - RCP in Operation

The P7 Automatic Inhibition - RCP in Operation permissive defines when RCPs are in operation.

The P7 Automatic Inhibition - RCP in Operation permissive is utilized in the following Functions:

– CVCS Isolation - ADM at Shutdown with RCP in Operation with Calculation, and
– CVCS Isolation - ADM at Shutdown with RCP in Operation.

Three divisions of the P7 Automatic Validation - RCP in Operation Function are required to be OPERABLE in MODE 5.

This Function utilizes the following sensors:

– RCP Breaker Position Indication sensors,
– RCP Bus Breaker Position Indication sensors, and
– RCP Speed sensors.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

To generate the permissive, when at least two of the following conditions are true, a signal is generated for that pump:

– RCP Breaker open position,
– RCP Bus Breaker open position,
– First RCP Speed measurement less than or equal to a setpoint (approximately 90%), and
– Second RCP Speed measurement less than or equal to a setpoint (approximately 90%).

When signals are generated for all four pumps, a delay time (approximately 600 seconds) is started. After the delay time has expired, the permissive is automatically validated. Otherwise, the permissive is inhibited.

7. P8 Automatic Validation

a. P8 Automatic Validation - Shutdown Rod Cluster Control Assembly (RCCA) Position Lower than Setpoint

The P8 permissive defines the shutdown state with all rods in (ARI).

The P8 Automatic Validation - Shutdown Rod Cluster Control Assembly (RCCA) Position Lower than Setpoint permissive is utilized is utilized in the following Functions:

– CVCS Isolation - ADM at Shutdown with RCP in Operation with Calculation, and
– CVCS Isolation - ADM at Shutdown with RCP in Operation.

Four divisions of the P8 Automatic Validation - Shutdown Rod Cluster Control Assembly (RCCA) Position Lower than Setpoint Function are required to be OPERABLE in MODE 3.

This Function utilizes the RCCA Shutdown Bank Analog Position Indication sensors.

To generate the permissive, each shutdown bank is composed of 12 RCCAs with 12 RCCA Shutdown Bank Bottom Position Indication sensors. RCCA Shutdown Bank Bottom Position Indication sensors are acquired in four different electrical divisions. For each division, when all rods in the shutdown banks are below 2 inches (5 steps), a signal is generated.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

8. P8 Automatic Inhibition

a. P8 Automatic Inhibition- Shutdown RCCA Position Higher than Setpoint

The P8 permissive defines the shutdown state with all rods in (ARI).

The P8 Automatic Inhibition- Shutdown RCCA Position Higher than Setpoint permissive is utilized in the following Functions:

– CVCS Isolation - ADM at Power with Calculation, and
– CVCS Isolation - ADM at Power.

Four divisions of the P8 Automatic Inhibition- Shutdown RCCA Position Higher than Setpoint Function are required to be OPERABLE in MODE 2.

The sensors utilized for this Function and its logic are described above in Function 7. a, P8 Automatic Validation - Shutdown Rod Cluster Control Assembly (RCCA) Position Lower than Setpoint.

9. P12 Manual Validation

a. P12 Manual Validation - Pressurizer Pressure Lower than Setpoint

The P12 permissive facilitates plant heat-up and cooldown by disabling certain ESF functions.

The P12 Manual Validation - Pressurizer Pressure Lower than Setpoint permissive is utilized in the ESF 1.b, SIS Actuation - Low Delta P_{sat} Function.

Four divisions of the P12 Manual Validation - Pressurizer Pressure Lower than Setpoint Function are required to be OPERABLE in MODE 3.

This Function utilizes the Pressurizer Pressure (Narrow Range) sensors.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

To generate the permissive, Pressurizer Pressure (Narrow Range) measurements are compared to the setpoint (approximately 2005 psia). When at least three measurements are less than the setpoint, the operator is prompted to manually validate the permissive.

b. P12 Manual Validation - Manual

The P12 permissive facilitates plant heat-up and cooldown by disabling certain ESF functions.

The P12 permissive facilitates plant heat-up and cooldown by disabling certain ESF functions.

The P12 Manual Validation - Manual permissive is utilized in the ESF 1.b: SIS Actuation - Low Delta P_{sat} Function.

Four divisions of the P12 Manual Validation - Manual Function are required to be OPERABLE in MODE 3.

P12 Manual Validation - Manual switches are available in the SICS in the Main Control Room. There is one switches per division.

When both the P12 Manual Validation - Pressurizer Pressure Lower than Setpoint and P12 Manual Validation - Manual signals are present, the permissive will be validated.

10. P12 Automatic Inhibition

a. P12 Automatic Inhibition - Pressurizer Pressure Higher than Setpoint

The P12 permissive facilitates plant heat-up and cooldown by disabling certain ESF functions.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

The P12 Automatic Inhibition - Pressurizer Pressure Higher than Setpoint permisisve is utilized in the following Functions:

– Reactor Trip 17: Pressurizer Level - High,
– Reactor Trip 18: Hot Leg Pressure - Low,
– Reactor Trip 20: SG Pressure - Low,
– ESF 1.a: SIS Actuation - Low Pressurizer Pressure,
– ESF 7.a: MSRT Isolation - Low SG Pressure (Affected SG),
– ESF 7.b: MSRT Isolation - Manual,
– ESF 8.b: Main Steam Isolation - Low SG Pressure (All SGs), and
– ESF 10.b: Startup and Shutdown System (SSS) Isolation - Low SG Pressure (Affected SG).

Four divisions of the P12 Automatic Inhibition - Pressurizer Pressure Higher than Setpoint Function are required to be OPERABLE in MODE 3.

The sensors utilized for this Function and its logic are described above in Function 9.a, P12 Manual Validation - Pressurizer Pressure Lower than Setpoint.

11. P13 Automatic Inhibition

a. P13 Automatic Inhibition - Hot Leg Temperature Higher than Setpoint

The P13 permissive defines when steam generator draining and filling operations are allowed.

The P13 Automatic Inhibition - Hot Leg Temperature Higher than Setpoint permisisve is utilized in the following Functions:

– Reactor Trip 22.a: SG Level - Low,
– Reactor Trip 22.b: SG Level - High,
– ESF 2.a: EFWS Actuation - Low-Low SG Level (Affected SG),
– ESF 2.b: EFWS Actuation - Manual (Affected SG),
– ESF 4.a: EFWS Isolation - High SG Level (Affected SG),
– ESF 4.b: EFWS Isolation - Manual,
– ESF 9.b: Main Feedwater Full Load Isolation - High SG Level (Affected SG),
– ESF 10.c: SSS Isolation - High SG Level for Period of Time (Affected SG), and
– ESF 12.a: SG Isolation - Manual.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

Four divisions of the P13 Automatic Inhibition - Hot Leg Temperature Higher than Setpoint Function are required to be OPERABLE in MODE 4.

This Function utilizes the Hot Leg Temperature (Wide Range) sensors.

To generate the permissive, Hot Leg Temperature (Wide Range) measurements are compared to the setpoint (approximately 200°F). When at least three measurements are less than the setpoint, the operator is prompted to manually validate the permissive. Otherwise, the permissive is inhibited.

12. P14 Manual Validation

a. P14 Manual Validation - Hot Leg Pressure and Hot Leg Temperature Lower than Setpoints

The P14 permissive defines when the residual heat removal system is allowed to be connected to the RCS.

The P14 Manual Validation - Hot Leg Pressure and Hot Leg Temperature Lower than Setpoints permisisve is utilized in the ESF 17.a: MHSI Large Miniflow Valves - Interlock Function.

Four divisions of the P14 Manual Validation - Hot Leg Pressure and Hot Leg Temperature Lower than Setpoints Function are required to be OPERABLE in MODE 4.

This Function utilizes the following sensors:

– Hot Leg Temperature (Wide Range), and
– Hot Leg Pressure (Wide Range).

To generate the permissive, Hot Leg Temperature (Wide Range) and Hot Leg Pressure (Wide Range) measurements are each compared to setpoints. When at least two Hot Leg Temperature (Wide Range) measurements are less than the temperature setpoint (approximately 350°F), and at least two Hot Leg Pressure (Wide Range) measurements are less than the pressure setpoint (approximately 464 psia), the operator is prompted to manually validate the permissive.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

b. P14 Manual Validation - Manual

The P14 permissive defines when the residual heat removal system is allowed to be connected to the RCS.

The P14 Manual Validation - Manual permissive is utilized in the ESF 17.a: MHSI Large Miniflow Valves - Interlock Function.

Four divisions of the P14 Manual Validation - Manual Function are required to be OPERABLE in MODE 4.

P14 Manual Validation - Manual switches are available in the SICS in the Main Control Room. There is one switches per division.

When both the P14 Manual Validation - Hot Leg Pressure and Hot Leg Temperature Lower than Setpoints and P14 Manual Validation - Manual signals are present, the permissive will be validated.

13. P14 Manual Inhibition

a. P14 Manual Inhibition - Hot Leg Pressure or Hot Leg Temperature Higher than Setpoints

The P14 permissive defines when the residual heat removal system is allowed to be connected to the RCS.

The P14 Manual Inhibition - Hot Leg Pressure and Hot Leg Temperature Lower than Setpoints permisisve is utilized in the ESF 5.a: Partial Cooldown Actuation - Automatic on SIS Actuation Function.

Four divisions of the P14 Manual Validation - Hot Leg Pressure and Hot Leg Temperature Lower than Setpoints Function are required to be OPERABLE in MODE 4.

The sensors utilized for this Function and its logic are described above in Function 12.a: P14 Manual Validation - Hot Leg Pressure and Hot Leg Temperature Lower than Setpoints.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

b. P14 Manual Inhibition - Manual

The P14 permissive defines when the residual heat removal system is allowed to be connected to the RCS.

The P14 Manual Inhibition - Manual permisisve is utilized in the ESF 5.a: Partial Cooldown Actuation - Automatic on SIS Actuation Function.

Four divisions of the P14 Manual Inhibition - Manual Function are required to be OPERABLE in MODE 4.

P14 Manual Inhibition - Manual switches are available in the SICS in the Main Control Room. There is one switch per division.

When both the P14 Manual Inhibition - Hot Leg Pressure and Hot Leg Temperature Lower than Setpoints and P14 Manual Inhibition - Manual signals are present, the permissive will be inhibited.

14. P15 Manual Validation

a. P15 Manual Validation - Hot Leg Pressure and Hot Leg Temperature Lower than Setpoints and No RCP in Operation

The P15 Manual Validation - Hot Leg Pressure and Hot Leg Temperature Lower than Setpoints and No RCP in Operation permissive defines when ESF 1.b: SIS Actuation - Low Delta P_{sat} is disabled and ESF 1.c: SIS Actuation - Low Hot Leg Loop Level is enabled.

The P15 Manual Validation - Hot Leg Pressure and Hot Leg Temperature Lower than Setpoints and No RCP in Operation permissive is utilized in the ESF 1.c: SIS Actuation - Low Hot Leg Loop Level Function.

Four divisions of the P15 Manual Validation - Hot Leg Pressure and Hot Leg Temperature Lower than Setpoints and No RCP in Operation Function are required to be OPERABLE in MODE 4. Three divisions are required to be OPERABLE in MODE 5.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

This Function utilizes the following sensors:

– Hot Leg Temperature (Wide Range),
– Hot Leg Pressure (Wide Range,
– RCP Breaker Position Indication,
– RCP Bus Breaker Position Indication, and
– RCP Speed sensors.

To generate the permissive, when at least two of the following conditions are true, a signal is generated for that pump:

– RCP Breaker open position,
– RCP Bus Breaker open position,
– First RCP Speed measurement less than or equal to a setpoint (approximately 90%), and
– Second RCP Speed measurement less than or equal to a setpoint (approximately 90%).

When signals are generated for all four pumps, a delay time (approximately 600 seconds) is started. After the delay time has expired, and at least three Hot Leg Temperature (Wide Range) measurements are less than the temperature setpoint (approximately 350°F), and at least three Hot Leg Pressure (Wide Range) measurements are less than the pressure setpoint (approximately 464 psia), the operator is prompted to manually validate the permissive.

b. P15 Manual Validation - Manual

The P15 Manual Validation - Manual permissive defines when ESF 1.b: SIS Actuation - Low Delta P_{sat} is disabled and ESF 1.c: SIS Actuation - Low Hot Leg Loop Level is enabled.

The P15 Manual Validation - Manual permisisve is utilized in the ESF 1.c: SIS Actuation - Low Hot Leg Loop Level Function.

Four divisions of the P15 Manual Validation - Manual Function are required to be OPERABLE in MODE 4. Three divisions are required to be OPERABLE in MODE 5.

P15 Manual Validation - Manual switches are available in the SICS in the Main Control Room. There is one switches per division.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

When both the P15 Manual Validation - Hot Leg Pressure and Hot Leg Temperature Lower than Setpoints and No RCP in Operation and P15 Manual Validation - Manual signals are present, the permissive will be validated.

15. P15 Automatic Inhibition

a. P15 Automatic Inhibition - Hot Leg Pressure or Hot Leg Temperature Higher than Setpoints or RCP in Operation

The P15 Automatic Inhibition - Hot Leg Pressure and Hot Leg Temperature Lower than Setpoints and No RCP in Operation permissive defines when ESF 1.b: SIS Actuation - Low Delta P_{sat} is disabled and ESF 1.c: SIS Actuation - Low Hot Leg Loop Level is enabled.

The P15 Automatic Inhibition - Hot Leg Pressure and Hot Leg Temperature Lower than Setpoints and No RCP in Operation permissive is utilized in the ESF 1.b: SIS Actuation - Low Delta P_{sat} Function.

Four divisions of the P15 Automatic Inhibition - Hot Leg Pressure and Hot Leg Temperature Lower than Setpoints and No RCP in Operation Function are required to be OPERABLE in MODE 4.

This Function utilizes the following sensors:

– Hot Leg Temperature (Wide Range),
– Hot Leg Pressure (Wide Range,
– RCP Breaker Position Indication,
– RCP Bus Breaker Position Indication, and
– RCP Speed sensors.

To generate the permissive, when at least two of the following conditions are true, a signal is generated for that pump:

– RCP Breaker open position,
– RCP Bus Breaker open position,
– First RCP Speed measurement less than or equal to a setpoint (approximately 90%), and
– Second RCP Speed measurement less than or equal to a setpoint (approximately 90%).

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

When signals are generated for all four pumps, a delay time (approximately 600 seconds) is started. After the delay time has expired, and at least three Hot Leg Temperature (Wide Range) measurements are less than the temperature setpoint (approximately 350°F), and at least three Hot Leg Pressure (Wide Range) measurements are less than the pressure setpoint (approximately 464 psia), the operator is prompted to manually validate the permissive. Otherwise, the permissive is inhibited.

16. P16 Manual Inhibition

a. P16 Manual Inhibition - Hot Leg Pressure Lower than Setpoint

The P16 permissive defines when Safety Injection may be aligned from the cold leg to the hot leg to mitigate the consequences of a LOCA.

Four divisions of the P16 Manual Inhibition - Hot Leg Pressure Lower than Setpoint Function are required to be OPERABLE in MODE 4.

This Function utilizes the Hot Leg Pressure (Wide Range) sensors.

To generate the permissive, Hot Leg Pressure (Wide Range) measurements are compared to the setpoint (approximately 290 psia). When at least two measurements are less than the setpoint, the operator is prompted to manually validate the permissive. Otherwise, the permissive is inhibited.

b. P16 Manual Inhibition - Manual

The P16 permissive defines when Safety Injection may be aligned from the cold leg to the hot leg to mitigate the consequences of a LOCA.

Four divisions of the P16 Manual Inhibition - Manual Function are required to be OPERABLE in MODE 4.

P16 Manual Inhibition - Manual switches are available in the SICS in the Main Control Room. There is one switches per division.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

When three Hot Leg Pressure (Wide Range) measurements are higher than the setpoint, a reactor trip reset signal is not present, and the operator manually inhibits the permissive; then P16 is inhibited.

17. P17 Manual Validation

a. P17 Manual Validation - Cold Leg Temperature Lower than Setpoint

The P17 permissive corresponds to the temperature conditions where brittle fracture protection is required.

The P17 Manual Validation - Cold Leg Temperature Lower than Setpoint Function is utilized in ESF 11.a: PSRV Opening – High Hot Leg Pressure Function.

Four divisions of the P17 Manual Validation - Cold Leg Temperature Lower than Setpoint Function are required to be OPERABLE in MODE 4 when MHSI Large Miniflow Valves and PSRV OPERABILITY are required by LCO 3.4.11, “Low Temperature Overpressure Protection (LTOP).”

This Function utilizes the Cold Leg Temperature (Wide Range) sensors.

To generate the permissive, Cold Leg Temperature (Wide Range) measurements are compared to the setpoint (approximately 248ºF). When at least three measurements are less than the setpoint, the operator is prompted to manually validate the permissive.

b. P17 Manual Validation - Manual

The P17 permissive corresponds to the temperature conditions where brittle fracture protection is required.

The P17 permissive is utilized in ESF 11.a: PSRV Opening – High Hot Leg Pressure Function.

Four divisions of the P17 Manual Validation - Manual Function are required to be OPERABLE in MODE 4 when MHSI Large Miniflow Valves and PSRV OPERABILITY are required by LCO 3.4.11, “Low Temperature Overpressure Protection (LTOP).”

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

P17 Manual Validation - Manual switches are available in the SICS in the Main Control Room. There is one switches per division.

When both the P17 Manual Validation - Cold Leg Temperature Lower than Setpoint and P17 Manual Validation - Manual signals are present, the permissive will be validated.

18. P17 Automatic Inhibition

a. P17 Automatic Inhibition - Cold Leg Temperature Lower than Setpoint

The P17 permissive corresponds to the temperature conditions where brittle fracture protection is required.

The P17 Automatic Inhibition - Cold Leg Temperature Lower than Setpoint Function is utilized in the CVCS Charging Line Isolation - High-High Pressurizer Level Function.

Four divisions of the P17 Automatic Inhibition - Cold Leg Temperature Lower than Setpoint Function are required to be OPERABLE in MODE 4.

The sensors utilized for this Function and its logic are described above in Function 17.a: P17 Manual Validation - Cold Leg Temperature Lower than Setpoint.

19. P18 Automatic Inhibition

a. P18 Automatic Inhibition - Hot Leg Temperature Higher than Setpoint and No Reactor Trip

The P18 permissive prevents the unsafe positioning of the SG transfer valves.

Four divisions of the P18 permissive function are required to be OPERABLE in MODE 4 when the SGs are relied upon for heat removal.

This Function utilizes the Hot Leg Temperature (Wide Range) sensors.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

To generate the permissive, Hot Leg Temperature (Wide Range) measurements are compared to the setpoint (approximately 194°F). When at least three measurements are less than the setpoint or a reactor trip is initiated, the permissive is automatically validated. Otherwise, the permissive is inhibited.

20. Actuation Logic

Four divisions of the Actuation Logic are required to be OPERABLE in MODES 1, 2, 3, and 4. Three divisions of the Actuation Logic are required to be OPERABLE in MODES 5 and 6.

This Function does not utilize any sensors.

The Permissive Instrumentation Functions satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

ACTIONS

The most common causes of division inoperability are outright failure or drift of the sensor sufficient to exceed the tolerance allowed by the plant specific setpoint analysis. Typically, the drift is found to be small and results in a delay of actuation rather than a total loss of function. This determination is generally made during the performance of a CALIBRATION when the sensor is set up for adjustment to bring it to within specification. If an as-found sensor calibration setting value is non-conservative with respect to the Allowable Value, the sensor is immediately declared inoperable, and the appropriate Condition(s) must be entered.

In the event that any sensor or function processor is found inoperable, then all affected Trip/ESF/Permissive Functions provided by that sensor or function processor must be declared inoperable, and the plant must enter any applicable Condition for the particular Trip/ESF/Permissive Function affected.

When the number of inoperable Functions exceeds that specified in Table 3.3.3-1, redundancy is lost and actions must be taken to restore the required redundancy.

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

BASES

ACTIONS (continued)

A.1

Condition A applies to all Permissive Instrumentation Functions. Condition A addresses the situation where one or more Functions with one or more divisions are inoperable. The Required Action is to refer to Table 3.3.3-1 and to take the Required Actions for the Functions affected. The Completion Times are those from the referenced Conditions and Required Actions.

B.1

Condition B applies when one Input & Acquisition Logic division is inoperable. In this condition, the minimum number of OPERABLE divisions to read the plant parameter, perform conditioning, calculations, compare the values to setpoints, and sending to the voting logic during an AOO or postulated accident coupled with a single failure is still available. Verification that the Actuation Logic voting has been modified ensures the Protection System reflects the condition. The Completion Time of 6 hours is reasonable considering the availability of automatic actuation and the low probability of an AOO or postulated accident occurring during this time.

C.1 and C.2

Condition C applies when one Input & Acquisition Logic division is inoperable. In this condition, the minimum number of OPERABLE divisions to read the plant parameter, perform conditioning, calculations, compare the values to setpoints, and sending to the voting logic during an AOO or postulated accident coupled with a single failure is still available. Verification that the Actuation Logic voting has been modified ensures the Protection System reflects the condition. The Completion Time of 6 hours is reasonable considering the availability of automatic actuation and the low probability of an AOO or postulated accident occurring during this time. The Completion Time of 72 hours is reasonable considering that there are two divisions available, the low probability of an event occurring during this interval, and the time necessary for repairs

D.1 and D.2

Condition D applies when two Input & Acquisition Logic divisions are inoperable. In this condition, the minimum number of OPERABLE

BASES

ACTIONS (continued)

divisions to read the plant parameter, perform conditioning, calculations, compare the values to setpoints, and sending to the voting logic during an AOO or postulated accident is still available.

For all Permissive Instrumentation Functions with two Input & Acquisition Logic divisions inoperable, verification that the Actuation Logic voting has been modified ensures the configuration of the Protection System logic reflects the plant condition. The Completion Time of 6 hours is reasonable considering the availability of automatic actuation and the low probability of an AOO or postulated accident occurring during this time. The Completion Time of 72 hours is reasonable considering that there are two OPERABLE Input & Acquisition Logic divisions, the low probability of an event occurring during this interval, and the time necessary for repairs.

E.1

Condition E addresses the failure of three or more Input & Acquisition Logic divisions or the inability to complete the remedial measures in the time allowed by Required Actions B.1, D.1, or D.2. In this condition, the P2 Automatic Validation – Power Range Flux Measurement Higher than First Setpoint Function is inoperable and the plant must be brought to a MODE in which the supported reactor trip functions are not required to be OPERABLE. To achieve this status, the plant must be brought to at least MODE 1 with P2 inhibited. The Completion Time of 4 hours 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.

F.1

Condition F addresses the failure of three or more Input & Acquisition Logic divisions or the inability to complete the remedial measures in the time allowed by Required Actions B.1, D.1, or D.2. In this condition, the P3 Automatic Validation - Power Range Flux Measurement Higher than Second Setpoint Function is inoperable and the plant must be brought to a MODE in which the supported reactor trip function is not required to be OPERABLE. To achieve this status, the plant must be brought to at least MODE 1 with P3 inhibited. The Completion Time of 2 hours 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.

BASES

ACTIONS (continued)

G.1

Condition G addresses the failure of three or more Input & Acquisition Logic divisions or the inability to complete the remedial measures in the time allowed by Required Actions B.1, D.1, or D.2. In this condition, the P5 Automatic Validation - Intermediate Range Flux Measurement Higher than Setpoint Function is inoperable and the plant must be brought to a MODE in which the supported reactor trip function is not required to be OPERABLE. To achieve this status, the plant must be brought to at least MODE 2 with P5 inhibited. The Completion Time of 6 hours is reasonable, based on operating experience, to reach the required plant conditions from MODE 2 in an orderly manner and without challenging plant systems.

H.1

Condition H addresses the failure of three or more Input & Acquisition Logic divisions or the inability to complete the remedial measures in the time allowed by Required Actions B.1, D.1, or D.2. In this condition, the P6 Automatic Inhibition - Thermal Core Power Lower than Setpoint Function is inoperable and the plant must be brought to a plant condition in which the supported reactor trip functions are not required to be OPERABLE. To achieve this status, actions must be taken to verify that P6 is validated. The Completion Time of 6 hours 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.

I.1

Condition I addresses the failure of two or more Input & Acquisition Logic divisions or the inability to complete the remedial measures in the time allowed by Required Actions C.1 or C.2. In this condition, P7 Automatic Validation - No RCPs in Operation is inoperable and the plant must be brought to a plant condition in which the supported ESFAS functions are not required to be OPERABLE. To achieve this status, actions must be taken to verify that P7 is inhibited. The Completion Time of 6 hours is reasonable, based on operating experience, to reach the required plant conditions from MODE 5 in an orderly manner and without challenging plant systems.

BASES

ACTIONS (continued)

J.1 and J.2

Condition J addresses the failure of two or more Input & Acquisition Logic divisions or the inability to complete the remedial measures in the time allowed by Required Actions C.1 or C.2. In this condition, P7 Automatic Inhibition - RCP in Operation is inoperable and operations involving positive reactivity addition that could result in loss of required shutdown margin or boron concentration must be suspended and actions initiated to restore required division(s) to OPERABLE status. The Completion Time of immediately is consistent with the required times for actions requiring prompt attention.

K.1

Condition K addresses the failure of three or more Input & Acquisition Logic divisions or the inability to complete the remedial measures in the time allowed by Required Actions B.1, D.1, or D.2. In this condition, the P8 Automatic Validation - Shutdown Rod Cluster Control Assembly (RCCA) Position Lower than Setpoint and P8 Automatic Inhibition-Shutdown RCCA Position Higher than Setpoint Functions are inoperable and the plant must be brought to a plant condition in which the supported reactor trip function is not required to be OPERABLE. To achieve this status, the plant must be brought to at least MODE 3 with P8 inhibited. The Completion Time of 6 hours is reasonable, based on operating experience, to reach the required plant conditions from MODE 3 in an orderly manner and without challenging plant systems.

L.1

Condition L addresses the failure of three or more Input & Acquisition Logic divisions or the inability to complete the remedial measures in the time allowed by Required Actions B.1, D.1, or D.2. In this condition, the P12 Manual Validation - Pressurizer Pressure Lower than Setpoint Function is inoperable and the plant must be brought to a plant condition in which the supported ESFAS functions are not required to be OPERABLE. To achieve this status, actions must be taken to verify that P12 is inhibited. The Completion Time of 6 hours is reasonable, based on operating experience, to reach the required plant conditions from MODE 3 in an orderly manner and without challenging plant systems.

BASES

ACTIONS (continued)

M.1

Condition M addresses the failure of three or more Input & Acquisition Logic divisions or the inability to complete the remedial measures in the time allowed by Required Actions B.1, D.1, or D.2. In this condition, the P12 Automatic Inhibition - Pressurizer Pressure Higher than Setpoint Function is inoperable and the plant must be brought to a plant condition in which the supported reactor trip and ESFAS functions are not required to be OPERABLE. To achieve this status, the plant must be brought to at least MODE 3 with P12 validated. The Completion Time of 6 hours is reasonable, based on operating experience, to reach the required plant conditions from MODE 3 in an orderly manner and without challenging plant systems.

N.1

Condition N addresses the failure of three or more Input & Acquisition Logic divisions or the inability to complete the remedial measures in the time allowed by Required Actions B.1, D.1, or D.2. In this condition, the P13 Automatic Inhibition - Hot Leg Temperature Higher than Setpoint Function is inoperable and the plant must be brought to a plant condition in which the supported reactor trip and ESFAS functions are not required to be OPERABLE. To achieve this status, the plant must be brought to at least MODE 4 without reliance upon steam generator for heat removal. The Completion Time of 24 hours to reach MODE 4 without reliance upon steam generator for heat removal is reasonable, based on operating experience, to reach the required plant conditions from MODE 4 in an orderly manner and without challenging plant systems.

O.1

Condition O addresses the failure of three or more Input & Acquisition Logic divisions or the inability to complete the remedial measures in the time allowed by Required Actions B.1, D.1, or D.2. In this condition, the P14 Manual Validation - Hot Leg Pressure and Hot Leg Temperature Lower than Setpoints Function is inoperable and the plant must be brought to a plant condition in which the supported ESFAS functions are not required to be OPERABLE. To achieve this status, actions must be taken to verify that P14 is inhibited. The Completion Time of 6 hours is reasonable, based on operating experience, to reach the required plant conditions from MODE 4 in an orderly manner and without challenging plant systems.

BASES

ACTIONS (continued)

P.1

Condition P addresses the failure of three or more Input & Acquisition Logic divisions or the inability to complete the remedial measures in the time allowed by Required Actions B.1, D.1, or D.2. In this condition, the P14 Manual Inhibition - Hot Leg Pressure or Hot Leg Temperature Higher than Setpoints Function is inoperable and the plant must be brought to a plant condition in which the supported ESFAS function is not required to be OPERABLE. To achieve this status, the plant must be brought to at least MODE 4 with P14 validated. The Completion Times of 24 hours to reach MODE 4 with P14 validated is reasonable, based on operating experience, to reach the required plant conditions from MODE 4 in an orderly manner and without challenging plant systems.

Q.1

Condition Q addresses the failure of three or more Input & Acquisition Logic divisions or the inability to complete the remedial measures in the time allowed by Required Actions B.1, D.1, or D.2. In this condition, the P15 Manual Validation - Hot Leg Pressure and Hot Leg Temperature Lower than Setpoints and No RCP in Operation Function is inoperable in MODE 4 and the plant must be brought to a plant condition in which the supported ESFAS function is not required to be OPERABLE. To achieve this status, actions must be taken to verify that P15 is inhibited. The Completion Time of 6 hours is reasonable, based on operating experience, to reach the required plant conditions from MODE 4 in an orderly manner and without challenging plant systems.

R.1

Condition R addresses the failure of two or more Input & Acquisition Logic divisions or the inability to complete the remedial measures in the time allowed by Required Actions B.1, C.1, or C.2. In this condition, the P15 Manual Validation - Hot Leg Pressure and Hot Leg Temperature Lower than Setpoints and No RCP in Operation Function is inoperable in MODE 5 and the plant must be brought to a plant condition in which the supported ESFAS function is not required to be OPERABLE. To achieve this status, actions must be taken to verify that P15 is inhibited. The Completion Time of 6 hours is reasonable, based on operating experience, to reach the required plant conditions from MODE 5 in an orderly manner and without challenging plant systems.

BASES

ACTIONS (continued)

S.1

Condition S addresses the failure of three or more Input & Acquisition Logic divisions or the inability to complete the remedial measures in the time allowed by Required Actions B.1, D.1, or D.2. In this condition, the P15 Automatic Inhibition - Hot Leg Pressure or Hot Leg Temperature Higher than Setpoints or RCP in Operation Function is inoperable and the plant must be brought to a plant condition in which the supported ESFAS function is not required to be OPERABLE. To achieve this status, actions must be taken to verify that P15 is validated. The Completion Time of 6 hours is reasonable, based on operating experience, to reach the required plant conditions from MODE 4 in an orderly manner and without challenging plant systems.

T.1

Condition T addresses the failure of three or more Input & Acquisition Logic divisions or the inability to complete the remedial measures in the time allowed by Required Actions B.1, D.1, or D.2. In this condition, the P16 Manual Inhibition - Hot Leg Pressure Lower than Setpoint Function is inoperable and the plant must be brought to a plant condition in which the supported ESFAS function is not required to be OPERABLE. To achieve this status, actions must be taken to verify that P16 is validated. The Completion Time of 6 hours is reasonable, based on operating experience, to reach the required plant conditions from MODE 4 in an orderly manner and without challenging plant systems..

U.1

Condition U addresses the failure of three or more Input & Acquisition Logic divisions or the inability to complete the remedial measures in the time allowed by Required Actions B.1, D.1, or D.2. In this condition, the P17 Manual Validation - Cold Leg Temperature Lower than Setpoint Function is inoperable and the plant must be brought to a plant condition in which the supported ESFAS functions are not required to be OPERABLE. To achieve this status, actions must be taken to verify that P17 is inhibited. The Completion Time of 6 hours is reasonable, based on operating experience, to reach the required plant conditions from MODE 4 in an orderly manner and without challenging plant systems..

BASES

ACTIONS (continued)

V.1

Condition V addresses the failure of three or more Input & Acquisition Logic divisions or the inability to complete the remedial measures in the time allowed by Required Actions B.1, D.1, or D.2. In this condition, the P17 Automatic Inhibition - Cold Leg Temperature Higher than Setpoint Function is inoperable and the plant must be brought to a plant condition in which the supported ESFAS function is not required to be OPERABLE. To achieve this status, actions must be taken to verify that P17 is validated. The Completion Time of 30 hours is reasonable, based on operating experience, to reach the required plant conditions from Mode 4 in an orderly manner and without challenging plant systems..

W.1, W.2, and W.3

Condition W addresses the failure of one Manual division or one Actuation Logic division.

Required Action W.1 is clarified by a Note that states it is only applicable to the following Functions:

1. P2 Automatic Validation,
2. P3 Automatic Validation,
3. P5 Automatic Validation,
4. P6 Automatic Inhibition,
10. P12 Automatic Inhibition, and
11. P13 Automatic Inhibition.

In this condition, the ability to automatically trip the reactor may have been impacted. The applicable Conditions and Required Actions of LCO 3.3.1, “Reactor Trip Instrumentation,” are required to be entered. The actions of LCO 3.3.1 provide adequate compensatory actions to assure plant safety. The Completion Time of immediately is consistent with the required times for actions requiring prompt attention.

Required Action W.2 is clarified by a Note that states it is only applicable to the following Functions:

9. P12 Manual Validation,
12. P14 Manual Validation,
13. P14 Manual Inhibition,
14. P15 Manual Validation,
15. P15 Automatic Inhibition,
16. P16 Manual Inhibition, and
17. P17 Manual Validation.

BASES

ACTIONS (continued)

In this condition, the ability to automatically actuate an ESF Function may have been impacted. The applicable Conditions and Required Actions of LCO 3.3.2, “ESFAS Instrumentation,” are required to be entered. The actions of LCO 3.3.2 provide adequate compensatory actions to assure plant safety. The Completion Time of immediately is consistent with the required times for actions requiring prompt attention.

Required Action W.3 is clarified by a Note that states it is only applicable to the following Functions:

5. P7 Automatic Validation,
6. P6 Automatic Inhibition,
7. P8 Automatic Validation,
8. P8 Automatic Inhibition, and
18. P17 Automatic Inhibition.

In this condition, the ability to automatically actuate an ESF Function may have been impacted. The applicable Conditions and Required Actions of LCO 3.3.5, “CVCS Instrumentation,” are required to be entered. The actions of LCO 3.3.5 provide adequate compensatory actions to assure plant safety. The Completion Time of immediately is consistent with the required times for actions requiring prompt attention.

SURVEILLANCE REQUIREMENTS

The SRs for each Function are identified by the Surveillance Requirements (SR) column of Table 3.3.3-1 for that Function. Most Functions are subject to CHANNEL CHECK, ACTUATION DEVICE OPERATIONAL TEST, CALIBRATION, SENSOR OPERATIONAL TEST, EXTENDED SELF TESTS, and RESPONSE TIME testing.

The SRs are modified by a Note. The Note directs the reader to Table 3.3.3-1 to determine the correct SRs to perform for each Function.

SR 3.3.3.1

Performance of the CHANNEL CHECK ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the 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

BASES

SURVEILLANCE REQUIREMENTS (continued)

CHECK will detect gross channel failure; therefore, it is key in verifying that the instrumentation continues to operate properly between each CALIBRATION.

Agreement criteria are determined by the plant staff, based on a combination of the channel instrument uncertainties, including isolation, indication, and readability. If a channel is outside the criteria, it may be an indication that the sensor or the signal processing equipment has drifted outside its limit. If the channels are within the criteria, it is an indication that the channels are OPERABLE.

The Frequency of 31 days is based on operating experience that demonstrates that channel failure is rare. The CHANNEL CHECK supplements less formal checks of channels during operational use of the displays associated with the LCO required channels.

SR 3.3.3.2

The incore – excore CALIBRATION for the Power Range indication consists of a normalization of the detector addressable constant multipliers based on a power calorimetric and flux map performed at or above 15% RTP. The Note to the SR states that the SR is not required to be performed until 24 hours after THERMAL POWER ≥ 15% RTP. At lower power levels, incore – excore calibration of the Power Range Detectors would be inaccurate. During a refueling startup calibrations performed at lower power levels should be verified against higher level flux maps and calibrated, if necessary, to ensure accurate power range performance.

If the absolute difference between the power range and incore measurements is greater than the allowable difference specified in the Setpoint Control Program, the power range channel is not inoperable, but an adjustment of the addressable constant multipliers is necessary to ensure that the incore measured axial offset agrees with the indicated excore axial offset. If the power range channel cannot be properly recalibrated, the channel is declared inoperable. The 31 day Frequency is adequate, considering that long term drift of the excore linear amplifiers is small, burnup of the detectors, and changes in axial offset are slow. Also, the excore readings are a strong function of the power produced in the peripheral fuel bundles, and do not represent an integrated reading across the core. The slow changes in neutron flux during the fuel cycle (radially and axially) can also be detected and incorporated in the periodic incore – excore CALIBRATION at this interval.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.3.3

A CALIBRATION of each RCS flow indication and calculation input every 24 months ensures that each instrument division is accurate and within the specified tolerance. This CALIBRATION consists of a normalization of the addressable constant multipliers based on RCS flow measured by a precision calorimetric (SR 3.4.1.4). If the absolute difference between the flow indication / calculation input and the value measured in the surveillance is greater than the allowable difference specified in the Setpoint Control Program, the flow indication / calculation input are not inoperable, but an adjustment of the addressable constant multipliers is necessary to ensure that the flow indication / calculation input agrees with measured RCS flow. If the RCS flow indication and calculation input cannot be properly recalibrated, the division is declared inoperable.

The Note to the SR states that the CALIBRATION is not required to be performed until 12 hours after THERMAL POWER ≥ 70% RTP. The RCS Flow Rate – Low-Low in One Loop trip function is required to be OPERABLE in MODE 1 with P3 permissive validated, which corresponds to this power level. The 24 month Frequency is adequate, considering that the RCS flow change over an operating cycle is small.

SR 3.3.3.4

A SENSOR OPERATIONAL TEST (SOT) is performed every 24 months to ensure the devices will perform their intended function when needed. The test is performed in accordance with the Setpoint Control Program.

A SOT shall be the injection of a simulated or actual signal into the division as close to the sensor as practicable to verify OPERABILITY of all devices in the division required for division OPERABILITY. The SOT shall include the verification of the accuracy and time constants of the analog input modules.

The SOT may be performed by means of any series of sequential, overlapping, or total steps.

SR 3.3.3.5

A CALIBRATION of each sensor every 24 months ensures that each instrument division is reading accurately and within tolerance. The test is performed in accordance with the Setpoint Control Program. A CALIBRATION shall be the adjustment, as necessary, of the sensor

BASES

SURVEILLANCE REQUIREMENTS (continued)

output such that it responds within the necessary range and accuracy to known values of the parameter that the division monitors. The CALIBRATION shall encompass all devices in the division required for sensor OPERABILITY.

The CALIBRATION includes provisions for the following:

1. Evaluation of sensor performance to verify that the sensor is functioning as required prior to returning the sensor to service if the as-found sensor calibration setting values are outside their predefined as-found tolerance for the specified calibration settings (e.g., 0, 25, 50, 75, and 100 percent), but conservative with respect to the Allowable Value, and

2. Declaring the sensor immediately inoperable if the sensor cannot be calibrated such that the as-left sensor calibration setting values are within the specified as-left tolerance around the specified calibration settings (e.g., 0, 25, 50, 75, and 100 percent), at the completion of the surveillance.

The CALIBRATION may be performed by means of any series of sequential, overlapping, or total steps.

SR 3.3.3.6

The features of continuous self-monitoring of the Protection System are described in Reference 1. Additional tests, which require the function processor to be inoperable are not normally performed during operation. These EXTENDED SELF TESTS are performed at start-up of a function processor each cycle. The startup sequence is as follows:

– Hardware basic test using the internal diagnosis monitor,
– Start-up self-test of the operating system, and
– Switch over to normal operation after approximately two minutes.

Additional information is provided in Section 2 of Reference 1.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.3.7

SR 3.3.3.7 is the performance of an ACTUATING DEVICE OPERATIONAL TEST (ADOT) every 24 months. The ADOT may be performed by means of any series of sequential, overlapping, or total steps.

SR 3.3.3.8

SR 3.3.3.8 verifies that the NTSPs have been properly loaded into the applicable APUs.

SR 3.3.3.9

Instrument Calibration

For intermediate range neutron flux channels, CALIBRATION is a complete check and readjustment of the channels, from the preamplifier input to the indicators. This test verifies the channel responds to a measured parameter within the necessary range and accuracy. CALIBRATION leaves the channel adjusted to account for instrument drift to ensure that the instrument channel remains operational between successive tests. There is a plant specific program which verifies that the instrument channel functions as required by verifying the as-left and as-found settings are consistent with those established by the setpoint methodology.

Setpoint Determination

Before each refueling startup determine the relative change in the peripheral assemblies when compared to the last time that the intermediate range setpoint (amps) was verified at the corresponding core power (percent power). Using the relative change for each assembly apply a weighting factor for a limited number of assemblies to calculate a new setpoint. The limited number of assemblies and the appropriate weighting factor is determined by a statistical analysis method (Monte Carlo). The analytical method determines the probability of a neutron that is born in any assembly reaching the intermediate range detector. For some assemblies like the center assembly in the core it is impossible to be born and survive long enough to get to the intermediate range

BASES

SURVEILLANCE REQUIREMENTS (continued)

detector. The setpoint calculation shall also account for things like replacing the detectors with a more sensitive model and changes in plant parameters, if necessary. During each startup (refueling or mid-cycle) the setpoint is verified when core power is equivalent to the intermediate range setpoint. If the absolute difference between the current intermediate range setpoint and the intermediate range current at the corresponding core power is greater than the allowable difference specified in the Setpoint Control Program, the intermediate range channel is not inoperable, but an adjustment of the addressable constant multipliers is necessary to ensure that the intermediate range measured current agrees with the desired intermediate setpoint. If the intermediate range channel cannot be properly recalibrated, the channel is declared inoperable. This intermediate range information can be used to make an adjustment to the setpoint, if necessary, and shall be used to calculate the next refueling setpoint.

General

The SR is modified by two Notes. The first Note requires the SR to be performed prior to withdrawing RCCAs for startup. The second Note excluding neutron detectors from CALIBRATION. It is not necessary to test the detectors because generating a meaningful test signal is difficult. In addition, the detectors are of simple construction, and any failures in the detectors will be apparent as a change in channel output. The Frequency is based on operating experience and consistency with the typical industry refueling cycle and is justified by demonstrated instrument reliability over a 24 month interval such that the instrument is not adversely affected by drift.

REFERENCES

1. ANP-10315P, Revision 1, “U.S. EPR Protection System Surveillance Testing and Teleperm XS Self-Monitoring Technical Report,” June 2011.

B 3.3 INSTRUMENTATION

B 3.3.4 Containment Isolation Instrumentation

BASES

BACKGROUND

Refer to B 3.3.1, “Reactor Trip Instrumentation,” for background information on the Distributed Control System. Refer to B 3.3.2, “Engineered Safety Feature Actuation System (ESFAS) Instrumentation,” for background information that is generically applicable to U.S. EPR systems that perform Engineered Safety Feature (ESF) functions.

Normally, there are four divisions of each ESF function, which utilize four divisions of Input & Acquisition Logic and Actuation Logic to actuate four division of equipment in four trains. The exception is the Containment Isolation Instrumentation, which only has one or two automatic isolation valves per containment penetration.

During a loss of coolant accident (LOCA), radioactive coolant is released into the containment. Therefore, the containment has to be isolated to prevent activity release to the environment. The U.S. EPR provides containment isolation in two stages to isolate nonessential components based on the size of the break. Containment pressure measurements and high-range activity monitors are used to initiate containment isolation and to determine which stage is actuated. Additionally, containment isolation is actuated anytime a safety injection actuation signal is generated.

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

Refer to B 3.3.2, “Engineered Safety Feature Actuation System (ESFAS) Instrumentation,” for applicable safety analyses, LCO, and applicability information that is generically applicable to U.S. EPR systems that perform ESF functions.

Stage 1 isolation is provided for a small break loss of coolant accident (SBLOCA) to isolate containment penetrations that have no active function for LOCA mitigation and to start ventilation of containment annulus. A LOCA of sufficient size to significantly raise containment pressure does not require reactor coolant pumps (RCP) for mitigation. On a stage 2 containment isolation signal, RCPs are tripped to limit energy input to containment, and containment penetrations for processes that support RCP operation are isolated.

In MODES 1, 2, 3, and 4, a design basis event could cause a release of radioactive material into containment and automatic isolation is required to mitigate the consequences. In MODES 5 and 6, the probability and

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

consequences of these events are reduced due to the pressure and temperature limitations of these MODES. Therefore, automatic containment isolation is not required to be OPERABLE in MODES 5 and 6 to prevent leakage of radioactive material from containment. However, manual isolation capability is provided as an added level of defense for reduced inventory conditions with fuel in the reactor vessel in the unlikely event of loss of core cooling.

LCO 3.3.4, “Containment Isolation Instrumentation,” addresses the following Functions:

1. Containment Isolation (Stage 1)

a. Containment Isolation (Stage 1) - Safety Injection Signal (SIS) Actuation

In case of the listed events, the containment has to be isolated in order to limit the release of radioactivity to the environment. This function mitigates the following postulated accidents or AOOs:

– Inadvertent opening of a pressurizer pilot operated safety valve, and
– LOCA.

Refer to LCO 3.3.2, “Engineered Safety Feature Actuation Systems (ESFAS) Instrumentation,” for OPERABILITY, ACTIONS, and Surveillance Requirements.

There is no NTSP associated with this Function.

There are no permissives associated with this Function.

b. Containment Isolation (Stage 1) - High Containment Pressure

In case of the listed events, the containment has to be isolated in order to limit the release of radioactivity to the environment. This function mitigates the following postulated accidents or AOOs:

– Inadvertent opening of a pressurizer pilot operated safety valve, and
– LOCA.

Four divisions of the Containment Isolation (Stage 1) - High Containment Pressure Function are required to be OPERABLE in MODES 1, 2, 3, and 4.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

This Function utilizes the following sensors:

– Containment Equipment Compartment Pressure sensors,
– Containment Service Compartment Pressure (Narrow Range) sensors, and
– Containment Service Compartment Pressure (Wide Range) sensors.

The NTSP is high enough to avoid spurious operation but low enough to ensure offsite dose consequences are maintained below 10 CFR 50.34 and 10 CFR 100.21 limits.

There are no permissives associated with this Function.

c. Containment Isolation (Stage 1) - High Containment Radiation

In case of the listed events, the containment has to be isolated in order to limit the release of radioactivity to the environment. This function mitigates the following postulated accidents or AOOs:

– Rod ejection,
– MSLB inside containment,
– Feedwater line break inside containment,
– Inadvertent opening of a pressurizer pilot operated safety valve, and
– LOCA.

Four divisions of the Containment Isolation (Stage 1) - High Containment Radiation Function are required to be OPERABLE in MODES 1, 2, 3, and 4.

This Function utilizes the Radiation Monitor - Containment High Range sensors.

The NTSP is high enough to avoid spurious operation but low enough to ensure offsite dose consequences are maintained below 10 CFR 50.34 and 10 CFR 100.21 limits.

There are no permissives associated with this function.

d. Containment Isolation (Stage 1) - Manual

Manual containment isolation capability is provided as an added level of defense for reduced inventory conditions with fuel in the reactor vessel in the unlikely event of loss of core cooling.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

Four divisions of the Containment Isolation (Stage 1) - Manual Function are required to be OPERABLE in MODES 1, 2, 3, and 4.
Three divisions of the Containment Isolation (Stage 1) - Manual Function are required to be OPERABLE for containment isolation valves providing direct access from the containment atmosphere to the outside atmosphere in MODE 5 when the RCS loops are not filled. Three divisions of the Containment Isolation (Stage 1) - Manual Function are required to be OPERABLE for containment isolation valves providing direct access from the containment atmosphere to the outside atmosphere in MODE 6 when the refueling cavity water level is less than 23 feet above the top of the reactor vessel flange.

Capability for manual system-level initiation of Containment Isolation (Stage 1) is provided on the SICS in the main control room (MCR). Four manual system-level isolation controls are provided. Any two of the four controls actuate containment isolation.

There are no permissives associated with this function.

2. Containment Isolation (Stage 2)

a. Containment Isolation (Stage 2) - High-High Containment Pressure

In case of the listed events, the containment has to be isolated in order to limit the release of radioactivity to the environment. This function mitigates the following postulated accidents or AOOs:

– Inadvertent opening of a pressurizer pilot operated safety valve, and
– LOCA.

Four divisions of the Containment Isolation (Stage 2) - High-High Containment Pressure Function are required to be OPERABLE in MODES 1, 2, 3, and 4.

This Function utilizes the Containment Service Compartment Pressure (Wide Range) sensors.

The NTSP is high enough to avoid spurious operation but low enough to ensure offsite dose consequences are maintained below 10 CFR 50.34 and 10 CFR 100.21 limits.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

d. Containment Isolation (Stage 2) - Manual

Manual containment isolation capability is provided as an added level of defense for reduced inventory conditions with fuel in the reactor vessel in the unlikely event of loss of core cooling.

Four divisions of the Containment Isolation (Stage 2) - Manual Function are required to be OPERABLE in MODES 1, 2, 3, and 4.

Capability for manual system-level initiation of Containment Isolation (Stage 2) is provided on the SICS in the MCR. Four manual system-level isolation controls are provided. Any two of the four controls actuate containment isolation.

There are no permissives associated with this function.

3. Actuation Logic

Four divisions of the Actuation Logic are required to be OPERABLE in MODES 1, 2, 3, and 4.

Three divisions of the Actuation Logic are required to be OPERABLE for containment isolation valves providing direct access from the containment atmosphere to the outside atmosphere in MODE 5 when the RCS loops are not filled. Three divisions of the Containment Isolation (Stage 1) - Manual Function are required to be OPERABLE for containment isolation valves providing direct access from the containment atmosphere to the outside atmosphere in MODE 6 when the refueling cavity water level is less than 23 feet above the top of the reactor vessel flange.

This Function does not utilize any sensors.

There is no NTSP associated with this Function.

There are no permissives associated with this Function.

ACTIONS

The most common causes of division inoperability are outright failure or drift of the sensor sufficient to exceed the tolerance allowed by the plant specific setpoint analysis. Typically, the drift is found to be small and results in a delay of actuation rather than a total loss of function. This determination is generally made during the performance of a CALIBRATION when the sensor is set up for adjustment to bring it to

BASES

ACTIONS (continued)

within specification. If an as-found sensor calibration setting value is non-conservative with respect to the Allowable Value, the sensor is immediately declared inoperable, and the appropriate Condition(s) must be entered.

In the event that any sensor or function processor is found inoperable, then all affected Trip/ESF/Permissive Functions provided by that sensor or function processor must be declared inoperable, and the plant must enter any applicable Condition for the particular Trip/ESF/Permissive Function affected.

When the number of inoperable Functions exceeds that specified in Table 3.3.4-1, redundancy is lost and actions must be taken to restore the required redundancy.

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

A.1

Condition A applies to all Containment Isolation Instrumentation Functions. Condition A addresses the situation where one or more Functions with one or more divisions are inoperable. The Required Action is to refer to Table 3.3.4-1 and to take the Required Actions for the Functions affected. The Completion Times are those from the referenced Conditions and Required Actions.

B.1

Condition B applies when one Input & Acquisition Logic division is inoperable. In this condition, the minimum number of OPERABLE divisions to read the plant parameter, perform conditioning, calculations, compare the values to setpoints, and sending to the voting logic during an AOO or postulated accident coupled with a single failure is still available. Verification that the Actuation Logic voting has been modified ensures the Protection System reflects the condition. The Completion Time of 6 hours is reasonable considering the availability of automatic actuation and the low probability of an AOO or postulated accident occurring during this time.

BASES

ACTIONS (continued)

C.1 and C.2

Condition C applies when two Input & Acquisition Logic divisions are inoperable. In this condition, the minimum number of OPERABLE divisions to read the plant parameter, perform conditioning, calculations, compare the values to setpoints, and sending to the voting logic during an AOO or postulated accident is still available.

For all Containment Isolation Instrumentation Functions with two Input & Acquisition Logic divisions inoperable, verification that the Actuation Logic voting has been modified ensures the configuration of the Protection System logic reflects the plant condition. The Completion Time of 6 hours is reasonable considering the availability of automatic actuation and the low probability of an AOO or postulated accident occurring during this time. The Completion Time of 72 hours to restore one Input & Acquisition Logic Division to OPERABLE status is reasonable considering that there are still two OPERABLE Input & Acquisition Logic divisions available, the low probability of an event occurring during this interval, and the time necessary for repairs.

D.1

Condition D applies when either one Manual division is inoperable or one Actuation Logic division is inoperable. In this condition, the remaining OPERABLE Actuating Logic division is still available to receive the partial trigger values from the Input & Acquisition Logic, provide further calculations, voting, logic and sending an actuation signal or the remaining Manual division is available to send an actuation signal.

The inoperable Manual division or Actuation Logic division must be restored to OPERABLE status within 72 hours. The Completion Time of 72 hours is reasonable considering that there is one Manual division or one Actuation Logic division available, the low probability of an event occurring during this interval, and the time necessary for repairs.

E.1

Condition E addresses the failure of three or more Input & Acquisition Logic divisions, multiple Manual or Actuation Logic divisions, or the inability to restore a failed division to OPERABLE status in the time allowed by Required Actions B.1, C.1, C.2 or D.1. In this condition, the ability to automatically isolate a containment penetration may have been impacted. The applicable Conditions and Required Actions of

BASES

ACTIONS (continued)

LCO 3.6.3, “Containment Isolation Valves,” are required to be entered for containment isolation valve(s) made inoperable by Containment Isolation Instrumentation. The actions of LCO 3.6.3, “Containment Isolation Valves,” provide adequate compensatory actions to assure plant safety. The Completion Time of immediately is consistent with the required times for actions requiring prompt attention.

F.1

Condition F applies when one or more required Manual division is inoperable. In this condition, the ability to automatic isolate a containment penetration may have been impacted. The applicable Conditions and Required Actions of LCO 3.9.7, “Containment Penetrations,” are required to be entered for containment isolation valve(s) made inoperable by Containment Isolation Instrumentation. The actions of LCO 3.9.7, “Containment Penetrations,” provide adequate compensatory actions to assure plant safety. The Completion Time of immediately is consistent with the required times for actions requiring prompt attention.

SURVEILLANCE REQUIREMENTS

The SRs for each Function are identified by the Surveillance Requirements (SR) column of Table 3.3.4-1 for that Function. Most Functions are subject to CHANNEL CHECK, ACTUATION DEVICE OPERATIONAL TEST, CALIBRATION, SENSOR OPERATIONAL TEST, EXTENDED SELF TESTS, and RESPONSE TIME testing.

The SRs are modified by a Note. The Note directs the reader to Table 3.3.4-1 to determine the correct SRs to perform for each Function.

SR 3.3.4.1

Performance of the CHANNEL CHECK ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the 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; therefore, it is key in verifying that the instrumentation continues to operate properly between each CALIBRATION.

BASES

SURVEILLANCE REQUIREMENTS (continued)

Agreement criteria are determined by the plant staff, based on a combination of the channel instrument uncertainties, including isolation, indication, and readability. If a channel is outside the criteria, it may be an indication that the sensor or the signal processing equipment has drifted outside its limit. If the channels are within the criteria, it is an indication that the channels are OPERABLE.

The Frequency of 31 days is based on operating experience that demonstrates that channel failure is rare. The CHANNEL CHECK supplements less formal checks of channels during operational use of the displays associated with the LCO required channels.

SR 3.3.4.2

A SENSOR OPERATIONAL TEST (SOT) is performed every 24 months to ensure the devices will perform their intended function when needed. The test is performed in accordance with the Setpoint Control Program. A SOT shall be the injection of a simulated or actual signal into the division as close to the sensor as practicable to verify OPERABILITY of all devices in the division required for division OPERABILITY. The SOT shall include the verification of the accuracy and time constants of the analog input modules.
The SOT may be performed by means of any series of sequential, overlapping, or total steps.

SR 3.3.4.3

A CALIBRATION of each sensor every 24 months ensures that each instrument division is reading accurately and within tolerance. The test is performed in accordance with the Setpoint Control Program. A CALIBRATION shall be the adjustment, as necessary, of the sensor output such that it responds within the necessary range and accuracy to known values of the parameter that the division monitors. The CALIBRATION shall encompass all devices in the division required for sensor OPERABILITY.

The CALIBRATION includes provisions for the following:

1. Evaluation of sensor performance to verify that the sensor is functioning as required prior to returning the sensor to service if the as-found sensor calibration setting values are outside their predefined as-found tolerance for the specified calibration settings (e.g., 0, 25,

BASES

SURVEILLANCE REQUIREMENTS (continued)

50, 75, and 100 percent), but conservative with respect to the Allowable Value, and

2. Declaring the sensor immediately inoperable if the sensor cannot be calibrated such that the as-left sensor calibration setting values are within the specified as-left tolerance around the specified calibration settings (e.g., 0, 25, 50, 75, and 100 percent), at the completion of the surveillance.

The CALIBRATION may be performed by means of any series of sequential, overlapping, or total steps.

SR 3.3.4.4

The features of continuous self-monitoring of the Protection System are described in Reference 1. Additional tests, which require the function processor to be inoperable are not normally performed during operation. These EXTENDED SELF TESTS are performed at start-up of a function processor each cycle. The startup sequence is as follows:

– Hardware basic test using the internal diagnosis monitor,
– Start-up self-test of the operating system, and
– Switch over to normal operation after approximately two minutes.

Additional information is provided in Section 2 of Reference 1.

SR 3.3.4.5

SR 3.3.4.5 is the performance of an ACTUATING DEVICE OPERATIONAL TEST (ADOT) every 24 months. The ADOT may be performed by means of any series of sequential, overlapping, or total steps.

SR 3.3.4.6

This surveillance verifies that the NTSPs have been properly loaded into the applicable APUs. The test is performed in accordance with the Setpoint Control Program.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.4.7

This surveillance verifies that the individual division actuation response times are less than or equal to the maximum values assumed in the accident analysis. Response time testing acceptance criteria are included in a document controlled under 10 CFR 50.59. Individual component response times are not modeled in the analyses.

The analyses model the overall or total elapsed time, from the point at which the parameter exceeds the trip setpoint value at the sensor to the point at which the equipment reaches the required functional state (e.g., valves in full closed position).

For divisions that include dynamic transfer functions (e.g., lag, lead/lag, rate/lag, etc.), the response time test may be performed with the transfer function set to one, with the resulting measured response time compared to the appropriate FSAR response time. Alternately, the response time test can be performed with the time constants set to their nominal value, provided the required response time is analytically calculated assuming the time constants are set at their nominal values. The response time may be measured by a series of overlapping tests such that the entire response time is measured.

----------REVIEWER'S NOTE----------
The following Bases apply to plants that have obtained NRC approval to utilize allocations for selected components based on NRC-approved U.S. EPR-applicable Topical Reports.

[Response time may be verified by actual response time tests in any series of sequential, overlapping or total division measurements, or by the summation of allocated sensor, signal processing and actuation logic response times with actual response time tests on the remainder of the division. Allocations for sensor response times may be obtained from: (1) historical records based on acceptable response time tests (hydraulic, noise, or power interrupt tests), (2) in place, onsite, or offsite (e.g., vendor) test measurements, or (3) utilizing vendor engineering specifications. NRC-approved U.S. EPR-applicable Topical Report provides the basis and methodology for using allocated sensor response times in the overall verification of the division response time for specific sensors identified in the report. Response time verification for other sensor types must be demonstrated by test.

BASES

SURVEILLANCE REQUIREMENTS (continued)

NRC-approved U.S. EPR-applicable Topical Report (provide reference) provides the basis and methodology for using allocated signal processing and actuation logic response times in the overall verification of the DCS division response time.

The allocations for sensor, signal conditioning, and actuation logic response times must be verified prior to placing the component in operational service and re-verified following maintenance that may adversely affect response time. In general, electrical repair work does not impact response time provided the parts used for repair are of the same type and value. One example where response time could be affected is replacing the sensing assembly of a transmitter.]

As appropriate, each division's response must be verified every 24 months on a STAGGERED TEST BASIS. Testing of the final actuation devices is included in the testing. Response times cannot be determined during plant operation because equipment operation is required to measure response times. Experience has shown that these components usually pass this surveillance when performed at the 24 month Frequency. Therefore, the Frequency was concluded to be acceptable from a reliability standpoint.

REFERENCES

1. ANP-10315P, Revision 1, "U.S. EPR Protection System Surveillance Testing and Teleperm XS Self-Monitoring Technical Report," June 2011.

B 3.3 INSTRUMENTATION

B 3.3.5 Chemical and Volume Control System (CVCS) Isolation Instrumentation

BASES

BACKGROUND

Refer to B 3.3.1, “Reactor Trip Instrumentation,” for background information on the Distributed Control System. Refer to B 3.3.2, “Engineered Safety Feature Actuation System (ESFAS) Instrumentation,” for background information that is generically applicable to U.S. EPR systems that perform Engineered Safety Feature (ESF) functions.

Normally, there are four divisions of each ESF function, which utilize four divisions of Input & Acquisition Logic and Actuation Logic. The exception is the CVCS Isolation Instrumentation, which only utilizes two divisions of Actuation Logic.

The CVCS Isolation Instrumentation supports the following Functions:

1. CVCS Charging Line Isolation

A malfunction of the CVCS could result in overfilling the pressurizer and opening of the pressurizer safety relief valves (PSRV). Isolation of the CVCS is therefore required when the pressurizer water level increases inadvertently. The isolation is performed by redundant isolation valves.

If two-out-of-four level measurements exceed the Max2p setpoint, orders are generated to isolate the CVCS charging flow and the auxiliary spray. These CVCS charging isolation Functions are bypassed when cold leg temperature is below the P17 permissive setpoint. The bypass is automatically removed above the P17 permissive setpoint. The capability for manual system-level initiation is provided. One manual system-level isolation control is provided for Protection System (PS) Division 1, and one control is provided for PS Division 4.

2. CVCS Isolation for Anti-Dilution

To mitigate the risk of dilution of the RCS boron concentration, a CVCS isolation is required to secure potential dilution flow paths. This Function provides protection during all plant conditions by using different combinations of input signals depending on the current plant state.

3. Actuation Logic

CVCS isolation is performed by redundant isolation valves.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

Refer to B 3.3.2, “Engineered Safety Feature Actuation System (ESFAS) Instrumentation,” for applicable safety analyses, LCO, and applicability information that is generically applicable to U.S. EPR systems that perform ESF functions.

LCO 3.3.5, “Chemical and Volume Control System (CVCS) Isolation Instrumentation,” addresses the following Functions:

1. CVCS Charging Line Isolation

The isolation of the CVCS Charging Isolation is required to avoid filling of the pressurizer and subsequent water overflow through the safety valves. This Function protects against a CVCS malfunction that causes an increase in RCS water inventory.

The CVCS Charging Line Isolation Functions are:

a. CVCS Charging Isolation on High-High Pressurizer Level

Four divisions of the CVCS Charging Isolation on High-High Pressurizer Level Instrumentation are required to be OPERABLE in:

– MODES 1, 2, 3, and
– MODE 4 with P17 permissive inhibited.

This Function utilizes the Pressurizer Level (Narrow Range) sensors. There is one Pressurizer Level (Narrow Range) sensor per division.

The Nominal Trip Setpoint (NTSP) is low enough to initiate appropriate mitigative actions in time to prevent the pressurizer from overfilling during the CVCS malfunction event that may increases RCS inventory, but high enough to prevent spurious operations.

Inhibition of the P17 permissive automatically enables the CVCS Charging Isolation on High-High Pressurizer Level Function when the cold leg temperature is greater than or equal to approximately 248°F. When below this threshold, the Function is disabled by manual validation of the P17 permissive.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

b. CVCS Charging Isolation - Manual

Two divisions (Divisions 1 and 4) of the CVCS Charging Isolation – Manual Instrumentation are required to be OPERABLE in MODES 1, 2, 3 and 4.

The capability for manual system-level initiation of CVCS charging isolation is provided on a per-division basis on the Safety Information and Control System (SICS) in the main control room (MCR). One manual system-level isolation control is provided for Division 1, and one control is provided for Division 4.

There is no NTSP associated with this Function.

There are no permissives associated with this Function.

2. CVCS Isolation

The CVCS Isolation Functions are:

a. CVCS Isolation on Anti-Dilution Mitigation (ADM) at Power

This Function mitigates a homogeneous dilution event at power conditions. This Function ensures that the dilution is stopped when the protection is actuated.

Four divisions of the CVCS Isolation on ADM at Power Instrumentation are required to be OPERABLE in:

– MODE 1, and
– MODE 2 with P8 permissive inhibited.

This Function utilizes the following sensors:

– Boron Concentration - CVCS Charging Line sensors (4 divisions),
– Boron Temperature - CVCS Charging Line sensors (4 divisions), and
– CVCS Charging Line Flow sensors (4 divisions).

The NTSP is low enough to provide an operating envelope that prevents unnecessary isolations but high enough to mitigate a dilution event at power.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

Inhibition of the P8 permissive automatically enables the CVCS Isolation on ADM at Power Function when the RCCA Shutdown Bank Analog Position Indication sensors show an RCCA is not inserted.

b. CVCS Isolation on ADM at Power with Calculation

This Function mitigates a homogeneous dilution event at power conditions. This Function ensures that the dilution is stopped when the protection is actuated.

Four divisions of the CVCS Isolation on ADM at Power with Calculation Instrumentation are required to be OPERABLE in:

– MODE 1, and
– MODE 2 with P8 permissive inhibited.

This Function utilizes the following sensors:

– Boron Concentration - CVCS Charging Line sensors (4 divisions),
– Boron Temperature - CVCS Charging Line sensors (4 divisions), and
– CVCS Charging Line Flow sensors (4 divisions).

The NTSP is low enough to provide an operating envelope that prevents unnecessary isolations but high enough to mitigate a dilution event at power.

Inhibition of the P8 permissive automatically enables the CVCS Isolation on ADM at Power Function when the RCCA Shutdown Bank Analog Position Indication sensors show an RCCA is not inserted.

c. CVCS Isolation on ADM at Shutdown with RCP in Operation

This Function mitigates a homogeneous dilution event in the standard shutdown conditions where the RCPs are in operation. This Function ensures that:

– The dilution is stopped when the protection is actuated, and
– The core remains sub-critical.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

Four divisions of the of the CVCS Isolation on ADM at Shutdown with RCP in Operation Instrumentation are required to be OPERABLE in MODES 3 and 4 with P7 permissive inhibited and P8 permissive validated. Three divisions are required to be OPERABLE in MODE 5 with P7 permissive inhibited and P8 permissive validated.

This Function utilizes the following sensors:

– Boron Concentration - CVCS Charging Line sensors (4 divisions),
– Boron Temperature - CVCS Charging Line sensors (4 divisions),
– CVCS Charging Line Flow sensors (4 divisions), and
– Cold Leg Temperature (Wide Range) sensors (4 divisions).

The NTSP is low enough to provide an operating envelope that prevents unnecessary isolations but high enough to mitigate a dilution event in the shutdown condition where the RCPs are in operation.

Inhibition of the P7 permissive and validation of the P8 permissive automatically enables the Function. When all RCCA Shutdown Bank Analog Position Indication sensors show the RCCAs are inserted, the Function is automatically enabled by validation of the P8 permissive. With one or more RCPs in operation, the Function is automatically enabled by inhibition of the P7 permissive.

d. CVCS Isolation on ADM at Shutdown with RCP in Operation with Calculation

This Function mitigates a homogeneous dilution event in the standard shutdown states where the RCPs are in operation. This Function ensures that:

– The dilution is stopped when the protection is actuated, and
– The core remains sub-critical.

Four divisions of the of the Input CVCS Isolation on ADM at Shutdown with RCP in Operation with Calculation Instrumentation are required to be OPERABLE in MODES 3 and 4 with P7

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

permissive inhibited and P8 permissive validated. Three divisions are required to be OPERABLE in MODE 5 with P7 permissive inhibited and P8 permissive validated.

This Function utilizes the following sensors:

– Boron Concentration - CVCS Charging Line sensors (4 divisions), and
– Boron Temperature - CVCS Charging Line sensors (4 divisions).

The NTSP is low enough to provide an operating envelope that prevents unnecessary isolations but high enough to mitigate a dilution event in the shutdown condition where the RCPs are in operation.

Inhibition of the P7 permissive and validation of the P8 permissive automatically enables the Function. When all RCCA Shutdown Bank Analog Position Indication sensors show the RCCAs are inserted, the Function is automatically enabled by validation of the P8 permissive. With one or more RCPs in operation, the Function is automatically enabled by inhibition of the P7 permissive.

e. CVCS Isolation on ADM at Shutdown with No RCP in Operation

This Function mitigates a dilution event where no RCPs are in operation. This Function ensures that:

– The dilution is stopped when the protection is actuated, and
– The core remains sub-critical.

Four divisions of the of the Input & Acquisition Logic are required to be OPERABLE in MODE 4 with P7 permissive validated. Three divisions of the Function are required to be OPERABLE in MODES 5 and 6 with P7 permissive validated.

This Function utilizes the following sensors:

– Boron Concentration - CVCS Charging Line sensors (4 divisions), and
– Boron Temperature - CVCS Charging Line sensors (4 divisions).

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

The NTSP is low enough to provide an operating envelope that prevents unnecessary isolations but high enough to mitigate a dilution event in the shutdown condition where the RCPs are not in operation.

Validation of the P7 permissive automatically enables the Function when all RCPs are not in operation. When any RCP is operating, the Function is automatically disabled by inhibition of the P7 permissive.

f. CVCS Isolation - Manual

The capability for manual system-level initiation of CVCS charging isolation is provided on a per-division basis on the SICS in the MCR. One manual system-level isolation control is provided for Division 1, and one control is provided for Division 4.

This Function mitigates any dilution event. This Function ensures that the dilution is stopped when the protection is manually actuated.

Two divisions (Divisions 1 and 4 only) of the CVCS Isolation – Manual Instrumentation are required to be OPERABLE in MODES 1, 2, 3 and 4. One division (Division 1 or 4) of the Function is required to be OPERABLE in MODES 5 and 6.

This Function utilizes two manual CVCS Isolation on ADM switches (Divisions 1 and 4) which are provided for on the SICS in the MCR.

There is no NTSP associated with this Function.

There are no permissives associated with this Function.

3. Actuation Logic

Two divisions of the CVCS Charging Line Isolation Actuation Logic (Divisions 1 and 4 only) are required to be OPERABLE in MODES 1, 2, 3 and 4. One division (Divisions 1 or 4) of the Function is required to be OPERABLE in MODE 5 and in Mode 6 with P7 Permissive validated.

This Function does not utilize any sensors.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

There is no NTSP associated with this Function.

There are no permissives associated with this Function.

The automatic CVCS Isolation Instrumentation Functions satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii). The manual CVCS Isolation Instrumentation Functions satisfy Criterion 4 of 10 CFR 50.36(c)(2)(ii).

ACTIONS

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

A.1

Condition A applies to all CVCS Isolation Functions. Condition A addresses the situation where one or more Functions with one or more required divisions are inoperable. The Required Action is to refer to Table 3.3.5-1 and to take the Required Actions for the Functions affected. The Completion Times are those from the referenced Conditions and Required Actions.

B.1

Condition B applies when one Input & Acquisition Logic division is inoperable. In this condition, the minimum number of OPERABLE divisions to read the plant parameter, perform conditioning, calculations, compare the values to setpoints, and sending to the voting logic during an AOO or postulated accident coupled with a single failure is still available. Verification that the Actuation Logic voting has been modified in the required divisions (Divisions 1 and 4) ensures the Protection System reflects the condition. The Completion Time of 6 hours is reasonable considering the availability of automatic actuation and the low probability of an AOO or postulated accident occurring during this time.

C.1 and C.2

Condition C applies when one required Input & Acquisition Logic division is inoperable. In this condition, the minimum required number of OPERABLE divisions to read the plant parameter, perform conditioning,

BASES

ACTIONS (continued)

calculations, compare the values to setpoints, and sending to the voting logic during an AOO or postulated accident coupled with a single failure is still available. Verification that the Actuation Logic voting has been modified in the required divisions (Divisions 1 and 4) ensures the configuration of the Protection System logic reflects the plant condition. The Completion Time of 6 hours is reasonable considering the availability of automatic actuation and the low probability of an AOO or postulated accident occurring during this time.

The inoperable Input & Acquisition Logic division must be restored to OPERABLE status. The Completion Time of 72 hours is reasonable considering that there are three OPERABLE Input & Acquisition Logic divisions, the low probability of an event occurring during this interval, and the time necessary for repairs.

D.1 and D.2

Condition D applies when two Input & Acquisition Logic divisions are inoperable. In this condition, the minimum number of OPERABLE divisions to read the plant parameter, perform conditioning, calculations, compare the values to setpoints, and sending to the voting logic during an AOO or postulated accident is still available. Verification that the Actuation Logic voting has been modified in the required divisions (Divisions 1 and 4) ensures the configuration of the Protection System logic reflects the plant condition.

One inoperable Input & Acquisition Logic division must be restored to OPERABLE status. The Completion Time of 72 hours is reasonable considering that there are two OPERABLE Input & Acquisition Logic divisions, the low probability of an event occurring during this interval, and the time necessary for repairs.

E.1

Condition E applies when either one Manual division is inoperable or one Actuation Logic division is inoperable. In this condition, the remaining OPERABLE Actuating Logic division is still available to receive the partial trigger values from the Input & Acquisition Logic, provide further calculations, voting, logic and sending an actuation signal or the remaining Manual division is available to send an actuation signal. The inoperable Manual division or Actuation Logic division must be restored to OPERABLE status. The Completion Time of 72 hours is reasonable

BASES

ACTIONS (continued)

The Completion Time of considering that there is one Manual division or one Actuation Logic division available, the low probability of an event occurring during this interval, and the time necessary for repairs.

F.1

Condition F addresses the failure of three or more Input & Acquisition Logic divisions, multiple Manual or Actuation Logic divisions, or the inability to restore a failed division to OPERABLE status in the time allowed by Required Actions B.1, D.1, D.2, or E.1. In this condition, the CVCS Volume Control Tank or letdown isolation valve(s) has been made inoperable. The applicable Conditions and Required Actions of LCO 3.1.8, “Anti-Dilution Mitigation” must be entered immediately since these actions minimize the probability of the occurrence of postulated events. The Completion Time of immediately is consistent with the required times for actions requiring prompt attention.

G.1

Condition G addresses the failure of three or more Input & Acquisition Logic divisions, multiple Manual or Actuation Logic divisions, or the inability to restore a failed division to OPERABLE status in the time allowed by Required Actions B.1, D.1, D.2, or E.1. In this condition, the CVCS charging line isolation valve(s) has been made inoperable. The applicable Conditions and Required Actions of LCO 3.4.9, “Pressurizer” must be entered immediately since these actions minimize the probability of the occurrence of postulated events. The Completion Time of immediately is consistent with the required times for actions requiring prompt attention.

H.1

Condition H addresses the failure of multiple required Input & Acquisition Logic divisions, one required Manual or Actuation Logic division, or the inability to restore a failed division to OPERABLE status in the time allowed by Required Actions C.1 or C.2. In this condition, the CVCS Volume Control Tank or letdown isolation valve(s) has been made inoperable. The applicable Conditions and Required Actions of LCO 3.1.8, “Anti-Dilution Mitigation” must be entered immediately since these actions minimize the probability of the occurrence of postulated events. The Completion Time of immediately is consistent with the required times for actions requiring prompt attention.

BASES

SURVEILLANCE REQUIREMENTS

The SRs for each Function are identified by the Surveillance Requirements (SR) column of Table 3.3.5-1 for that Function. Most Functions are subject to CHANNEL CHECK, ACTUATION DEVICE OPERATIONAL TEST, CALIBRATION, SENSOR OPERATIONAL TEST, EXTENDED SELF TESTS, and RESPONSE TIME testing.

The SRs are modified by a Note. The Note directs the reader to Table 3.3.5-1 to determine the correct SRs to perform for each Function.

SR 3.3.5.1

Performance of the CHANNEL CHECK ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the 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; therefore, it is key in verifying that the instrumentation continues to operate properly between each CALIBRATION.

Agreement criteria are determined by the plant staff, based on a combination of the channel instrument uncertainties, including isolation, indication, and readability. If a channel is outside the criteria, it may be an indication that the sensor or the signal processing equipment has drifted outside its limit. If the channels are within the criteria, it is an indication that the channels are OPERABLE.
The Frequency of 31 days is based on operating experience that demonstrates that channel failure is rare. The CHANNEL CHECK supplements less formal checks of channels during operational use of the displays associated with the LCO required channels.

SR 3.3.5.2

The online boron meters are a half shell design and are not in contact with the reactor coolant. The concentration of boron is measured by using the neutron absorption effect of B-10. The boron concentration is calculated using the measured count rate. To improve the accuracy of the measurement, the temperature of the reactor coolant at the measuring point is used to adjust the boron concentration. The boron meter is used to protect against an inadvertent dilution, including the introduction of natural boron to the reactor coolant system.

BASES

SURVEILLANCE REQUIREMENTS (continued)

This calibration will be performed with the boron concentration and enrichment information that is collected and used to perform SR 3.1.2.1. These instruments aren't able to distinguish between changes in enrichment and changes in concentration. This surveillance adjusts constant multipliers to reduce the difference between the concentration measured by the boron meter and the results obtained by titration. In a similar manner this surveillance adjusts constant multipliers to reduce the difference between the enrichment measured by the boron meter and the results obtained by a mass spectrometer. If the absolute difference between the indicated boron concentration / enrichment and the measured values of these parameters is greater than the allowable difference specified in the Setpoint Control Program, the boron meter is not inoperable, but an adjustment of the addressable constant multipliers is necessary to ensure that the boron meter indication agrees with the independently measured values.

The temperature instruments are not included as part of this Surveillance. The frequency of the boron meter CALIBRATION is conservative considering instrument reliability.

SR 3.3.5.3

A SENSOR OPERATIONAL TEST (SOT) is performed every 24 months to ensure the devices will perform their intended function when needed. The test is performed in accordance with the Setpoint Control Program. A SOT shall be the injection of a simulated or actual signal into the division as close to the sensor as practicable to verify OPERABILITY of all devices in the division required for division OPERABILITY. The SOT shall include the verification of the accuracy and time constants of the analog input modules.

The SOT may be performed by means of any series of sequential, overlapping, or total steps.

SR 3.3.5.4

A CALIBRATION of each sensor every 24 months ensures that each instrument division is reading accurately and within tolerance. The test is performed in accordance with the Setpoint Control Program. A CALIBRATION shall be the adjustment, as necessary, of the sensor output such that it responds within the necessary range and accuracy to known values of the parameter that the division monitors. The CALIBRATION shall encompass all devices in the division required for sensor OPERABILITY.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The CALIBRATION includes provisions for the following:

1. Evaluation of sensor performance to verify that the sensor is functioning as required prior to returning the sensor to service if the as-found sensor calibration setting values are outside their predefined as-found tolerance for the specified calibration settings (e.g., 0, 25, 50, 75, and 100 percent), but conservative with respect to the Allowable Value, and

2. Declaring the sensor immediately inoperable if the sensor cannot be calibrated such that the as-left sensor calibration setting values are within the specified as-left tolerance around the specified calibration settings (e.g., 0, 25, 50, 75, and 100 percent), at the completion of the surveillance.

The CALIBRATION may be performed by means of any series of sequential, overlapping, or total steps. The temperature instruments are included as part of this Surveillance.

SR 3.3.5.5

The features of continuous self-monitoring of the Protection System are described in Reference 1. Additional tests, which require the function processor to be inoperable are not normally performed during operation. These EXTENDED SELF TESTS are performed at start-up of a function processor each cycle. The startup sequence is as follows:

– Hardware basic test using the internal diagnosis monitor,
– Start-up self-test of the operating system, and
– Switch over to normal operation after approximately two minutes.

Additional information is provided in Section 2 of Reference 1.

SR 3.3.5.6

SR 3.3.5.6 is the performance of an ACTUATING DEVICE OPERATIONAL TEST (ADOT) every 24 months. The ADOT may be performed by means of any series of sequential, overlapping, or total steps.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.5.7

This surveillance verifies that the NTSPs have been properly loaded into the applicable APUs. The test is performed in accordance with the Setpoint Control Program.

SR 3.3.5.8

This surveillance verifies that the individual division actuation response times are less than or equal to the maximum values assumed in the accident analysis. Response time testing acceptance criteria are included in a document controlled under 10 CFR 50.59. Individual component response times are not modeled in the analyses.

The analyses model the overall or total elapsed time, from the point at which the parameter exceeds the trip setpoint value at the sensor to the point at which the equipment reaches the required functional state (e.g., valves in full closed position).

For divisions that include dynamic transfer functions (e.g., lag, lead/lag, rate/lag, etc.), the response time test may be performed with the transfer function set to one, with the resulting measured response time compared to the appropriate FSAR response time. Alternately, the response time test can be performed with the time constants set to their nominal value, provided the required response time is analytically calculated assuming the time constants are set at their nominal values. The response time may be measured by a series of overlapping tests such that the entire response time is measured.

----------REVIEWER'S NOTE----------
The following Bases apply to plants that have obtained NRC approval to utilize allocations for selected components based on NRC-approved U.S. EPR-applicable Topical Reports.

[Response time may be verified by actual response time tests in any series of sequential, overlapping or total division measurements, or by the summation of allocated sensor, signal processing and actuation logic response times with actual response time tests on the remainder of the division. Allocations for sensor response times may be obtained from: (1) historical records based on acceptable response time tests (hydraulic, noise, or power interrupt tests), (2) in place, onsite, or offsite (e.g., vendor) test measurements, or (3) utilizing vendor engineering

BASES

SURVEILLANCE REQUIREMENTS (continued)

specifications. NRC-approved U.S. EPR-applicable Topical Report provides the basis and methodology for using allocated sensor response times in the overall verification of the division response time for specific sensors identified in the report. Response time verification for other sensor types must be demonstrated by test.

NRC-approved U.S. EPR-applicable Topical Report (provide reference) provides the basis and methodology for using allocated signal processing and actuation logic response times in the overall verification of the DCS division response time.

The allocations for sensor, signal conditioning, and actuation logic response times must be verified prior to placing the component in operational service and re-verified following maintenance that may adversely affect response time. In general, electrical repair work does not impact response time provided the parts used for repair are of the same type and value. One example where response time could be affected is replacing the sensing assembly of a transmitter.]

As appropriate, each division's response must be verified every 24 months on a STAGGERED TEST BASIS. Testing of the final actuation devices is included in the testing. Response times cannot be determined during plant operation because equipment operation is required to measure response times. Experience has shown that these components usually pass this surveillance when performed at the 24 month Frequency. Therefore, the Frequency was concluded to be acceptable from a reliability standpoint.

REFERENCES

1. ANP-10315P, Revision 1, "U.S. EPR Protection System Surveillance Testing and Teleperm XS Self-Monitoring Technical Report," June 2011.

B 3.3 INSTRUMENTATION

B 3.3.6 Reactor Coolant Pump (RCP) Trip Instrumentation

BASES

BACKGROUND

Refer to B 3.3.1, “Reactor Trip Instrumentation,” for background information on the Distributed Control System. Refer to B 3.3.2, “Engineered Safety Feature Actuation System (ESFAS) Instrumentation,” for background information that is generically applicable to U.S. EPR systems that perform Engineered Safety Feature (ESF) functions.

Normally, there are four divisions of each ESF function, which utilize four divisions of Input & Acquisition Logic and Actuation Logic. The actuated equipment for the instrumentation is governed by other LCOs. The exception is the Reactor Coolant Pump (RCP) Trip Instrumentation, whose actuated instrumentation is included with the Instrumentation LCO.

RCPs are tripped when conditions indicate that two-phase flow is present. This is done because the RCPs may subsequently be lost due to cavitation or operation in a degraded environment. Forced convection of the two-phase flow increases the mass lost via the break. If the RCPs are permitted to operate for an extended period of time in this condition and then are shut down, an inadequate core cooling condition may occur due to insufficient liquid inventory as the two phases separate. For this reason, an automatic RCP pump trip is provided early after two phase flow is indicated, while the void fraction is still relatively low, to enhance long term accident mitigation and minimize the potential for RCS mass depletion.

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

Refer to B 3.3.2, “Engineered Safety Feature Actuation System (ESFAS) Instrumentation,” for applicable safety analyses, LCO, and applicability information that is generically applicable to U.S. EPR systems that perform ESF functions.

In case of a loss of coolant accident (LOCA) in combination with a Safety Injection Signal (SIS) actuation or the inadvertent opening of a Pressurizer Safety Valve, the RCPs are tripped to prevent their operation in scenarios where timing of the pump trip is related to maintaining core cooling. When a Containment Isolation (Stage 2) signal is generated, the RCPs are tripped to prevent their operation in scenarios where the cooling water and seal water are isolated to the RCPs.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

The Reactor Coolant Pump (RCP) Trip Instrumentation supports the following Functions:

1. RCP Trip

a. RCP Trip - Low Delta Pressure across RCP and SIS Actuation for a Period of Time

This Function mitigates the following postulated accidents or AOOs:

– Inadvertent opening of a Pressurizer Safety Relief Valve, and
– Small break LOCA.

Four divisions of this Function are required to be OPERABLE in MODES 1, 2, 3, and 4.

This Function utilizes the RCP Delta Pressure sensors. The sensors required to generate the SIS actuation signal are identified in B 3.3.2, “Engineered Safety Feature Actuation System (ESFAS) Instrumentation,” under each separate ESF Function: SIS on Low Pressurizer Pressure, SIS Actuation on Low Delta P_{sat}, and SIS Actuation on Low Hot Leg Loop Level.

The NTSP is low enough to avoid spurious operation but high enough to ensure core cooling is maintained.

There are no permissives associated with this Function.

b. RCP Trip - Manual

This Function mitigates the following postulated accidents or AOOs:

– Inadvertent opening of a Pressurizer Safety Relief Valve,
– Small break LOCA,
– Inadvertent opening of a pressurizer pilot operated safety valve, and
– LOCA.

Four divisions of this Function are required to be OPERABLE in MODES 1, 2, 3, and 4.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

The capability for manual system-level RCP trip on a per-pump basis is provided to the operator on the Safety Information and Control System in the main control room. Two system-level initiation controls are provided for each pump. Either of the controls will trip the desired RCP.

There is no NTSP associated with this Function.

There are no permissives associated with this Function.

2. RCP Breakers

This Function mitigates the following postulated accidents or AOOs:

– Inadvertent opening of a Pressurizer Safety Relief Valve,
– Small break LOCA,
– Inadvertent opening of a pressurizer pilot operated safety valve, and
– LOCA.

Four divisions of this Function are required to be OPERABLE in MODES 1, 2, 3, and 4.

This Function utilizes two RCP Trip Breakers per division, which are provided for each RCP. Either of the breakers will trip the desired RCP. When the conditions for RCP trip are satisfied, orders are issued to open the circuit breakers that supply power to each RCP. When the orders are issued, a time delay begins. The time delay logic block is used to delay the opening of the redundant RCP circuit breaker so that simultaneous opening of RCP circuit breakers does not cause an excessive voltage surge. When the time delay expires, an order is issued to trip the corresponding bus supply circuit breaker upstream of the RCP circuit breaker to remove power from the RCP.

There is no NTSP associated with this Function.

There are no permissives associated with this Function.

3. Actuation Logic

Four divisions of the RCP Trip Actuation are required to be OPERABLE in MODES 1, 2, 3 and 4.

This Function does not utilize any sensors.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

There is no NTSP associated with this Function.

There are no permissives associated with this Function.

The automatic RCP Trip Isolation Instrumentation Functions satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii). The manual RCP Trip Isolation Instrumentation Function satisfies Criterion 4 of 10 CFR 50.36(c)(2)(ii).

ACTIONS

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

A.1

Condition A applies to all RCP Trip Instrumentation Functions. Condition A addresses the situation where one or more Functions with one or more divisions are inoperable. The Required Action is to refer to Table 3.3.6-1 and to take the Required Actions for the Functions affected. The Completion Times are those from the referenced Conditions and Required Actions.

B.1

Condition B applies when one Input & Acquisition Logic division is inoperable. In this condition, the minimum number of OPERABLE divisions to read the plant parameter, perform conditioning, calculations, compare the values to setpoints, and sending to the voting logic during an AOO or postulated accident coupled with a single failure is still available. Verification that the Actuation Logic voting has been modified ensures the Protection System reflects the condition. The Completion Time of 6 hours is reasonable considering the availability of automatic actuation and the low probability of an AOO or postulated accident occurring during this time.

BASES

ACTIONS (continued)

C.1 and C.2

Condition C applies when two Input & Acquisition Logic divisions are inoperable. In this condition, the minimum number of OPERABLE divisions to read the plant parameter, perform conditioning, calculations, compare the values to setpoints, and sending to the voting logic during an AOO or postulated accident is still available. Verification that the Actuation Logic voting has been modified ensures the configuration of the Protection System logic reflects the plant condition. The Completion Time of 6 hours is reasonable considering the availability of automatic actuation and the low probability of an AOO or postulated accident occurring during this time.

One inoperable Input & Acquisition Logic division must be restored to OPERABLE status. The Completion Time of 72 hours is reasonable considering that there are two OPERABLE Input & Acquisition Logic divisions, the low probability of an event occurring during this interval, and the time necessary for repairs.

D.1

Condition D applies when one RCP inoperable. In this condition, the remaining RCP Breaker for that pump is still available to interrupt power to the RCP. The Completion Time of 72 hours is reasonable considering that there is at least one RCP Breaker available for each pump, the low probability of an event occurring during this interval, and the time necessary for repairs.

E.1

Condition E applies when either one Manual division is inoperable or one Actuation Logic division is inoperable. In this condition, the remaining OPERABLE Actuation Logic division is still available to receive the partial trigger values from the Input & Acquisition Logic, provide further calculations, voting, logic and sending an actuation signal or the remaining Manual division is available to send an actuation signal.

The inoperable Manual division or Actuation Logic division must be restored to OPERABLE status within 72 hours. The Completion Time of 72 hours is reasonable considering that there is one Manual division or one Actuation Logic division available, the low probability of an event occurring during this interval, and the time necessary for repairs.

BASES

ACTIONS (continued)

F.1 and F.2

Condition F addresses the failure of three or more Input & Acquisition Logic divisions; both RCP Breakers for one or more RCP Pumps; multiple Manual or Actuation Logic divisions, or the inability to restore a failed division to OPERABLE status in the time allowed by Required Actions B.1, C.1, C.2, D.1, or E.1. The plant must be brought to a MODE where the LCO is no longer applicable.

The Completion Time of 6 hours to reach MODE 3 and 36 hours to reach MODE 5 is reasonable, based on operating experience, to reach the required MODES from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

The SRs for each Function are identified by the Surveillance Requirements (SR) column of Table 3.3.6-1 for that Function. Most Functions are subject to CHANNEL CHECK, ACTUATION DEVICE OPERATIONAL TEST, CALIBRATION, SENSOR OPERATIONAL TEST, EXTENDED SELF TESTS, and RESPONSE TIME testing.

The SRs are modified by a Note. The Note directs the reader to Table 3.3.6-1 to determine the correct SRs to perform for each Function.

SR 3.3.6.1

Performance of the CHANNEL CHECK ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the 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; therefore, it is key in verifying that the instrumentation continues to operate properly between each CALIBRATION.

Agreement criteria are determined by the plant staff, based on a combination of the channel instrument uncertainties, including isolation, indication, and readability. If a channel is outside the criteria, it may be an indication that the sensor or the signal processing equipment has drifted outside its limit. If the channels are within the criteria, it is an indication that the channels are OPERABLE.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The Frequency of 31 days is based on operating experience that demonstrates that channel failure is rare. The CHANNEL CHECK supplements less formal checks of channels during operational use of the displays associated with the LCO required channels.

SR 3.3.6.2

A SENSOR OPERATIONAL TEST (SOT) is performed every 24 months to ensure the devices will perform their intended function when needed. The test is performed in accordance with the Setpoint Control Program. A SOT shall be the injection of a simulated or actual signal into the division as close to the sensor as practicable to verify OPERABILITY of all devices in the division required for division OPERABILITY. The SOT shall include the verification of the accuracy and time constants of the analog input modules.

The SOT may be performed by means of any series of sequential, overlapping, or total steps.

SR 3.3.6.3

A CALIBRATION of each sensor every 24 months ensures that each instrument division is reading accurately and within tolerance. The test is performed in accordance with the Setpoint Control Program. A CALIBRATION shall be the adjustment, as necessary, of the sensor output such that it responds within the necessary range and accuracy to known values of the parameter that the division monitors. The CALIBRATION shall encompass all devices in the division required for sensor OPERABILITY.

The CALIBRATION includes provisions for the following:

1. Evaluation of sensor performance to verify that the sensor is functioning as required prior to returning the sensor to service if the as-found sensor calibration setting values are outside their predefined as-found tolerance for the specified calibration settings (e.g., 0, 25, 50, 75, and 100 percent), but conservative with respect to the Allowable Value, and

2. Declaring the sensor immediately inoperable if the sensor cannot be calibrated such that the as-left sensor calibration setting values are within the specified as-left tolerance around the specified calibration settings (e.g., 0, 25, 50, 75, and 100 percent), at the completion of the surveillance.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The CALIBRATION may be performed by means of any series of sequential, overlapping, or total steps.

SR 3.3.6.4

The features of continuous self-monitoring of the Protection System are described in Reference 1. Additional tests, which require the function processor to be inoperable are not normally performed during operation. These EXTENDED SELF TESTS are performed at start-up of a function processor each cycle. The startup sequence is as follows:

– Hardware basic test using the internal diagnosis monitor,
– Start-up self-test of the operating system, and
– Switch over to normal operation after approximately two minutes.

Additional information is provided in Section 2 of Reference 1.

SR 3.3.6.5

SR 3.3.6.5 is the performance of an ACTUATING DEVICE OPERATIONAL TEST (ADOT) every 24 months. The ADOT may be performed by means of any series of sequential, overlapping, or total steps.

SR 3.3.6.6

This surveillance verifies that the NTSPs have been properly loaded into the applicable APUs. The test is performed in accordance with the Setpoint Control Program.

SR 3.3.6.7

This surveillance verifies that the individual division actuation response times are less than or equal to the maximum values assumed in the accident analysis. Response time testing acceptance criteria are included in a document controlled under 10 CFR 50.59. Individual component response times are not modeled in the analyses.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The analyses model the overall or total elapsed time, from the point at which the parameter exceeds the trip setpoint value at the sensor to the point at which the equipment reaches the required functional state (e.g., breaker in the open position).

For divisions that include dynamic transfer functions (e.g., lag, lead/lag, rate/lag, etc.), the response time test may be performed with the transfer function set to one, with the resulting measured response time compared to the appropriate FSAR response time. Alternately, the response time test can be performed with the time constants set to their nominal value, provided the required response time is analytically calculated assuming the time constants are set at their nominal values. The response time may be measured by a series of overlapping tests such that the entire response time is measured.

----------REVIEWER'S NOTE----------
The following Bases apply to plants that have obtained NRC approval to utilize allocations for selected components based on NRC-approved U.S. EPR-applicable Topical Reports.

[Response time may be verified by actual response time tests in any series of sequential, overlapping or total division measurements, or by the summation of allocated sensor, signal processing and actuation logic response times with actual response time tests on the remainder of the division. Allocations for sensor response times may be obtained from: (1) historical records based on acceptable response time tests (hydraulic, noise, or power interrupt tests), (2) in place, onsite, or offsite (e.g., vendor) test measurements, or (3) utilizing vendor engineering specifications. NRC-approved U.S. EPR-applicable Topical Report provides the basis and methodology for using allocated sensor response times in the overall verification of the division response time for specific sensors identified in the report. Response time verification for other sensor types must be demonstrated by test.

NRC-approved U.S. EPR-applicable Topical Report (provide reference) provides the basis and methodology for using allocated signal processing and actuation logic response times in the overall verification of the DCS division response time.

The allocations for sensor, signal conditioning, and actuation logic response times must be verified prior to placing the component in operational service and re-verified following maintenance that may adversely affect response time. In general, electrical repair work does not

BASES

SURVEILLANCE REQUIREMENTS (continued)

impact response time provided the parts used for repair are of the same type and value. One example where response time could be affected is replacing the sensing assembly of a transmitter.]

As appropriate, each division's response must be verified every 24 months on a STAGGERED TEST BASIS. Testing of the final actuation devices is included in the testing. Response times cannot be determined during plant operation because equipment operation is required to measure response times. Experience has shown that these components usually pass this surveillance when performed at the 24 month Frequency. Therefore, the Frequency was concluded to be acceptable from a reliability standpoint.

REFERENCES

1. ANP-10315P, Revision 1, "U.S. EPR Protection System Surveillance Testing and Teleperm XS Self-Monitoring Technical Report," June 2011.

B 3.3 INSTRUMENTATION

B 3.3.7 Control Room Emergency Filtration (CREF) Instrumentation

BASES

BACKGROUND

Refer to B 3.3.1, “Reactor Trip Instrumentation,” for background information on the Distributed Control System. Refer to B 3.3.2, “Engineered Safety Feature Actuation System (ESFAS) Instrumentation,” for background information that is generically applicable to U.S. EPR systems that perform Engineered Safety Feature (ESF) functions.

Normally, there are four divisions of each ESF function, which utilize four divisions of Input & Acquisition Logic and Actuation Logic. The instrumentation normally actuates the Function using a two-out-of-four voting logic. The exception is the CREF Instrumentation, which actuates the CREF Function using a one-out-of-four logic.

The main control room air conditioning system (CRACS) is designed to maintain a controlled environment in the control room envelope (CRE) area for the comfort and safety of control room personnel and to support operability of the control room components during normal operation, anticipated operational occurrences and design basis accidents. Under normal operating conditions, the control room air conditioning system operates with fresh outside air (bypasses the control room emergency filtration (CREF) trains. During a site radiological contamination event, the fresh air intake is redirected through the CREF iodine filtration trains.

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

Refer to B 3.3.2, “Engineered Safety Feature Actuation System (ESFAS) Instrumentation,” for applicable safety analyses, LCO, and applicability information that is generically applicable to U.S. EPR systems that perform ESF functions.

The CRACS intakes are located on the roof of Safeguard Buildings 2 and 3. Radiation monitors in the CRACS supply air duct continuously measure the concentration of radioactive materials in the supply air. During a site radiological contamination event (i.e., rod ejection, loss of coolant accident, steam generator tube rupture, line breaks outside containment, and a fuel handling accident), the air intake is redirected through the ESF filter system trains when actuated by the CREF Instrumentation. All trains of the Main Control Room Air Conditioning System are reconfigured to ensure 10 CFR 50.34 limits are not exceeded.

The CREF Instrumentation supports the following Functions:

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

1. Control Room Emergency Filtration (CREF)

a. CREF on High Intake Activity

This Function mitigates the following postulated accidents or AOOs:

– Rod ejection,
– Loss of Coolant Accidents,
– Steam Generator Tube Rupture,
– Line Breaks Outside Containment, and
– Fuel handling accidents. (Bergeron to confirm – Not listed in Table 4-3)

Four divisions of this Function are required to be OPERABLE in MODES 1, 2, 3, and 4. Three divisions are required to be OPERABLE in MODES 5 and 6, and during movement of irradiated fuel assemblies.

This Function utilizes the Radiation Monitor - Control Room HVAC Intake Activity sensors.

The NTSP is high enough to avoid spurious operation but low enough to ensure offsite dose consequences are maintained below 10 CFR 50.34 limits.

There are no permissives associated with this Function.

b. CREF - Manual

This Function mitigates the following postulated accidents or AOOs:

– Rod ejection,
– Loss of Coolant Accidents,
– Steam Generator Tube Rupture,
– Line Breaks Outside Containment, and
– Fuel handling accidents. (Bergeron to confirm – Not listed in Table 4-3)

Two divisions of the CREF – Manual (Divisions 2 and 3 only) are required to be OPERABLE in MODES 1, 2, 3 and 4. One division (Division 2 or 3) is required to be OPERABLE in MODES 5 and 6, and during movement of irradiated fuel assemblies.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

The capability for manual system-level initiation of this function is provided on the Safety Information and Control System in the main control room. Two manual system-level initiation controls are provided, any one of which reconfigures both air intake paths.

There is no NTSP associated with this Function.

There are no permissives associated with this Function.

2. Actuation Logic

Four divisions of the CREF Actuation Logic are required to be OPERABLE in MODES 1, 2, 3 and 4. Three divisions are required to be OPERABLE in MODES 5 and 6, and during movement of irradiated fuel assemblies.

This Function does not utilize any sensors.

There is no NTSP associated with this Function.

There are no permissives associated with this Function.

The CREF on High Intake Activity Instrumentation Function satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii) in MODES 1, 2, 3, 4, 5 and 6 and during movement of irradiated fuel assemblies. (Bergeron to confirm) The CREF on Containment Isolation Instrumentation Function and CREF - Manual function satisfy Criterion 4 of 10 CFR 50.36(c)(2)(ii).

ACTIONS

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

A.1

Condition A applies to all CREF Instrumentation Functions. Condition A addresses the situation where one or more Functions with one or more required divisions are inoperable. The Required Action is to refer to Table 3.3.7-1 and to take the Required Actions for the Functions affected. The Completion Times are those from the referenced Conditions and Required Actions.

BASES

ACTIONS (continued)

B.1

Condition B applies when one Input & Acquisition Logic, one Manual, or Actuation Logic division is inoperable. In this condition, the minimum number of OPERABLE divisions to read the plant parameter, perform conditioning, calculations, compare the values to setpoints, and sending to the voting logic during an AOO or postulated accident coupled with a single failure is still available. The inoperable Input & Acquisition Logic, Manual, or Actuation Logic division must be restored to OPERABLE status within 72 hours. The Completion Time of 72 hours is reasonable considering that there is one remaining OPERABLE Input & Acquisition Logic, Manual, or Actuation Logic division available to reconfigure the effected train, the low probability of an event occurring during this interval, and the time necessary for repairs.

C.1, C.2 and C.3

Condition C applies when two or more Input & Acquisition Logic, two Manual, two or more Actuation Logic divisions are inoperable, or the Required Action and Completion Time or Condition B.1 is not met. With the CREF Instrumentation Function inoperable, the Required Actions are to immediately place both CREF trains in emergency mode, suspend movement of irradiated fuel assemblies, and to initiate action to restore one division to OPERABLE status. The Completion Time of immediately is consistent with the required times for actions requiring prompt attention.

D.1, D.2 and D.3

Condition D applies when one or more required Input & Acquisition Logic divisions are inoperable, one required Manual division is inoperable, or one or more required Actuation Logic divisions are inoperable. With the CREF Instrumentation Function inoperable, the Required Actions are to immediately place both CREF trains in emergency mode, suspend movement of irradiated fuel assemblies, and to initiate action to restore one division to OPERABLE status. The Completion Time of immediately is consistent with the required times for actions requiring prompt attention.

SURVEILLANCE REQUIREMENTS

The SRs for each Function are identified by the Surveillance Requirements (SR) column of Table 3.3.7-1 for that Function. Most Functions are subject to CHANNEL CHECK, ACTUATION DEVICE OPERATIONAL TEST, CALIBRATION, SENSOR OPERATIONAL TEST, EXTENDED SELF TESTS, and RESPONSE TIME testing.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The SRs are modified by a Note. The Note directs the reader to Table 3.3.7-1 to determine the correct SRs to perform for each Function.

SR 3.3.7.1

Performance of the CHANNEL CHECK ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the 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; therefore, it is key in verifying that the instrumentation continues to operate properly between each CALIBRATION.

Agreement criteria are determined by the plant staff, based on a combination of the channel instrument uncertainties, including isolation, indication, and readability. If a channel is outside the criteria, it may be an indication that the sensor or the signal processing equipment has drifted outside its limit. If the channels are within the criteria, it is an indication that the channels are OPERABLE.

The Frequency of 31 days is based on operating experience that demonstrates that channel failure is rare. The CHANNEL CHECK supplements less formal checks of channels during operational use of the displays associated with the LCO required channels.

SR 3.3.7.2

A SENSOR OPERATIONAL TEST (SOT) is performed every 24 months to ensure the devices will perform their intended function when needed. The test is performed in accordance with the Setpoint Control Program. A SOT shall be the injection of a simulated or actual signal into the division as close to the sensor as practicable to verify OPERABILITY of all devices in the division required for division OPERABILITY. The SOT shall include the verification of the accuracy and time constants of the analog input modules.

The SOT may be performed by means of any series of sequential, overlapping, or total steps.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.7.3

A CALIBRATION of each sensor every 24 months ensures that each instrument division is reading accurately and within tolerance. The test is performed in accordance with the Setpoint Control Program. A CALIBRATION shall be the adjustment, as necessary, of the sensor output such that it responds within the necessary range and accuracy to known values of the parameter that the division monitors. The CALIBRATION shall encompass all devices in the division required for sensor OPERABILITY.

The CALIBRATION includes provisions for the following:

1. Evaluation of sensor performance to verify that the sensor is functioning as required prior to returning the sensor to service if the as-found sensor calibration setting values are outside their predefined as-found tolerance for the specified calibration settings (e.g., 0, 25, 50, 75, and 100 percent), but conservative with respect to the Allowable Value, and

2. Declaring the sensor immediately inoperable if the sensor cannot be calibrated such that the as-left sensor calibration setting values are within the specified as-left tolerance around the specified calibration settings (e.g., 0, 25, 50, 75, and 100 percent), at the completion of the surveillance.

The CALIBRATION may be performed by means of any series of sequential, overlapping, or total steps.

SR 3.3.7.4

The features of continuous self-monitoring of the Protection System are described in Reference 1. Additional tests, which require the function processor to be inoperable are not normally performed during operation. These EXTENDED SELF TESTS are performed at start-up of a function processor each cycle. The startup sequence is as follows:

– Hardware basic test using the internal diagnosis monitor,
– Start-up self-test of the operating system, and
– Switch over to normal operation after approximately two minutes.

Additional information is provided in Section 2 of Reference 1.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.7.5

SR 3.3.7.5 is the performance of an ACTUATING DEVICE OPERATIONAL TEST (ADOT) every 24 months. The ADOT may be performed by means of any series of sequential, overlapping, or total steps.

SR 3.3.7.6

This surveillance verifies that the NTSPs have been properly loaded into the applicable APUs. The test is performed in accordance with the Setpoint Control Program.

SR 3.3.7.7

This surveillance verifies that the individual division actuation response times are less than or equal to the maximum values assumed in the accident analysis. Response time testing acceptance criteria are included in a document controlled under 10 CFR 50.59. Individual component response times are not modeled in the analyses.

The analyses model the overall or total elapsed time, from the point at which the parameter exceeds the trip setpoint value at the sensor to the point at which the equipment reaches the required functional state (e.g., dampers in full open or closed position).

For divisions that include dynamic transfer functions (e.g., lag, lead/lag, rate/lag, etc.), the response time test may be performed with the transfer function set to one, with the resulting measured response time compared to the appropriate FSAR response time. Alternately, the response time test can be performed with the time constants set to their nominal value, provided the required response time is analytically calculated assuming the time constants are set at their nominal values. The response time may be measured by a series of overlapping tests such that the entire response time is measured.

----------REVIEWER'S NOTE----------
The following Bases apply to plants that have obtained NRC approval to utilize allocations for selected components based on NRC-approved U.S. EPR-applicable Topical Reports.

BASES

SURVEILLANCE REQUIREMENTS (continued)

[Response time may be verified by actual response time tests in any series of sequential, overlapping or total division measurements, or by the summation of allocated sensor, signal processing and actuation logic response times with actual response time tests on the remainder of the division. Allocations for sensor response times may be obtained from: (1) historical records based on acceptable response time tests (hydraulic, noise, or power interrupt tests), (2) in place, onsite, or offsite (e.g., vendor) test measurements, or (3) utilizing vendor engineering specifications. NRC-approved U.S. EPR-applicable Topical Report provides the basis and methodology for using allocated sensor response times in the overall verification of the division response time for specific sensors identified in the report. Response time verification for other sensor types must be demonstrated by test.

NRC-approved U.S. EPR-applicable Topical Report (provide reference) provides the basis and methodology for using allocated signal processing and actuation logic response times in the overall verification of the DCS division response time.

The allocations for sensor, signal conditioning, and actuation logic response times must be verified prior to placing the component in operational service and re-verified following maintenance that may adversely affect response time. In general, electrical repair work does not impact response time provided the parts used for repair are of the same type and value. One example where response time could be affected is replacing the sensing assembly of a transmitter.]

As appropriate, each division's response must be verified every 24 months on a STAGGERED TEST BASIS. Testing of the final actuation devices is included in the testing. Response times cannot be determined during plant operation because equipment operation is required to measure response times. Experience has shown that these components usually pass this surveillance when performed at the 24 month Frequency. Therefore, the Frequency was concluded to be acceptable from a reliability standpoint.

REFERENCES

1. ANP-10315P, Revision 1, "U.S. EPR Protection System Surveillance Testing and Teleperm XS Self-Monitoring Technical Report," June 2011.

B 3.3 INSTRUMENTATION

B 3.3.8 Emergency Diesel Generator (EDG) Actuation Instrumentation

BASES

BACKGROUND

Refer to B 3.3.1, “Reactor Trip Instrumentation,” for background information on the Distributed Control System. Refer to B 3.3.2, “Engineered Safety Feature Actuation System (ESFAS) Instrumentation,” for background information that is generically applicable to U.S. EPR systems that perform Engineered Safety Feature (ESF) functions.

Normally, there are four divisions of each ESF function, which utilize four divisions of Input & Acquisition Logic and Actuation Logic. The instrumentation normally actuates the Function using a two-out-of-four voting logic.

The EDG actuation function is implemented in the PS architecture differently than the remainder of the ESF actuation functions. The three phases of voltage measurement for any one electrical division are acquired by the corresponding Protection System (PS) division. The processing and actuation of the related EDG are also carried out completely within the same PS division. For the actuation of any one EDG, redundancy within the PS is obtained by utilizing the functionally independent subsystems within each division. Both sub-systems within a division acquire the voltage measurements and either sub-system can actuate the same EDG.

The three phases of voltage on each main medium voltage bus are monitored by the PS to detect either a degraded voltage condition or a loss of voltage condition. If the voltage measurements for two of the three phases on a bus fall below a fixed setpoint for a fixed amount of time and a Safety Injection System (SIS) signal is received, a degraded voltage condition exists. After this fixed amount of time, if the voltage measurements for two of the three phases on a bus stay below the same fixed setpoint for an additional fixed amount of time without an SIS, a degraded voltage condition exists. If the voltage measurements for two of the three phases on a bus fall below a lower fixed setpoint for a fixed amount of time, a loss of voltage condition exists. In these cases, a loss of offsite power (LOOP) signal is generated within the PS which starts the corresponding EDG and begins the loading sequence. All four EDGs are also started automatically when a safety injection signal is generated, but they are not connected to the emergency power supply system unless a LOOP signal is also generated. The LOOP start actuation is described in FSAR, Section 7.3 (Ref. 1).

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

Refer to B 3.3.2, “Engineered Safety Feature Actuation System (ESFAS) Instrumentation,” for applicable safety analyses, LCO, and applicability information that is generically applicable to U.S. EPR systems that perform ESF functions.

The LOOP EDG start instrumentation is required for the Engineered Safety Features (ESF) Systems to function in any accident with a loss of offsite power. Its design basis is that of the ESF Actuation System (ESFAS).

Accident analyses credit the loading of the EDG based on the loss of offsite power during a loss of coolant accident (LOCA). The actual EDG start has historically been associated with the ESFAS actuation. The EDG loading has been included in the delay time associated with each safety system component requiring EDG supplied power following a loss of offsite power. The analyses assume a non-mechanistic EDG loading, which does not explicitly account for each individual component of loss of power detection and subsequent actions.

The required channels of LOOP EDG start instrumentation, in conjunction with the ESF systems powered from the EDGs, provide unit protection in the event of any of the analyzed accidents discussed in Reference 2, in which a loss of offsite power is assumed.

The delay times assumed in the safety analysis for the ESF equipment include the 15 second EDG start delay, and the appropriate sequencing delay, if applicable. The response times for ESFAS actuated equipment in LCO 3.3.2, "Engineered Safety Feature Actuation System (ESFAS) Instrumentation," includes the appropriate EDG loading and sequencing delay.

The EDG Actuation Instrumentation supports the following Functions:

1. EDG Actuation

a. EDG Actuation on Degraded Grid Voltage

This function mitigates a LOOP, which is assumed to occur independently or concurrently with postulated accidents and AOOs. This function ensures AC Power is available to mitigate postulated accidents and AOOs.

Four divisions of this Function are required to be OPERABLE in MODES 1, 2, 3, and 4. Two divisions in the same divisional pair (i.e., Divisions 1 and 2 or Divisions 3 and 4) are required to be OPERABLE in MODES 5 and 6, and during movement of irradiated fuel assemblies.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

This Function utilizes the 6.9 kV Bus Voltage sensors.

The NTSP is low enough to avoid spurious operation but high enough to ensure that power is provided to ESF functions in the time-frame assumed in the accident analyses.

There are no permissives associated with this Function.

b. EDG Actuation on Loss of Voltage

Following a loss of voltage on one 6.9 kV bus, the EDG associated with that bus is automatically started. This function mitigates a LOOP, which is assumed to occur independently or concurrently with postulated accidents and AOOs. This function ensures AC Power is available to mitigate postulated accidents and AOOs.

Four divisions of this Function are required to be OPERABLE in MODES 1, 2, 3, and 4. Two divisions in the same divisional pair (i.e., Divisions 1 and 2 or Divisions 3 and 4) are required to be OPERABLE in MODES 5 and 6, and during movement of irradiated fuel assemblies.

This Function utilizes the 6.9 kV Bus Voltage sensors.

The NTSP is low enough to avoid spurious operation but high enough to ensure that power is provided to ESF functions in the time-frame assumed in the accident analyses.

There are no permissives associated with this Function.

c. EDG Actuation on Safety Injection Signal Actuation

Following an SIS Actuation, the EDGs are automatically started. This function ensures AC Power is available to mitigate postulated accidents and AOOs.

This Function are required to be OPERABLE in MODES 1, 2, 3, 4, 5, and 6, and during movement of irradiated fuel assemblies.

The sensors, permissives, and NTSPs associated with the generation of SIS Actuation signals are identified under each separate automatic ESF function (i.e., 1.a, 1.b, and 1.c).

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

d. EDG Actuation - Manual

Following manual initiation, the EDG associated with that division is automatically started. This function mitigates a LOOP, which is assumed to occur independently or concurrently with postulated accidents and AOOs. This function ensures AC Power is available to mitigate postulated accidents and AOOs.

Four divisions of this Function are required to be OPERABLE in MODES 1, 2, 3, and 4. Two divisions in the same divisional pair (i.e., Divisions 1 and 2 or Divisions 3 and 4) are required to be OPERABLE in MODES 5 and 6, and during movement of irradiated fuel assemblies.

The capability for manual system-level start-up of EDGs on a per-EDG basis is provided on the Safety Information and Control System in the main control room. Two manual system-level controls are provided per EDG. Either of the two controls starts the desired EDG.

There is no NTSP associated with this Function.

There are no permissives associated with this Function.

2. Actuation Logic

Four divisions of the EDG Actuation Logic are required to be OPERABLE in MODES 1, 2, 3 and 4. Two divisions in the same divisional pair (i.e., Divisions 1 and 2 or Divisions 3 and 4) are required to be OPERABLE in MODES 5 and 6, and during movement of irradiated fuel assemblies.

This Function does not utilize any sensors.

There is no NTSP associated with this Function.

There are no permissives associated with this Function.

The EDG Actuation Instrumentation Functions satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii) in MODES 1, 2, 3, 4, 5 and 6 and during movement of irradiated fuel assemblies.

BASES

ACTIONS

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

A.1

Condition A applies to all EDG Actuation Instrumentation Functions. Condition A addresses the situation where one or more Functions with one or more required divisions are inoperable. The Required Action is to immediately enter the applicable Conditions and Required Actions of LCO 3.8.1, "AC Sources – Operating," or LCO 3.8.2, "AC Sources - Shutdown" for EDG made inoperable by EDG Actuation instrumentation. The purpose of each referenced action is addressed in the Bases for these sections. The Completion Time of immediately is consistent with the required times for actions requiring prompt attention.

SURVEILLANCE REQUIREMENTS

The SRs for each Function are identified by the Surveillance Requirements (SR) column of Table 3.3.8-1 for that Function. Most Functions are subject to CHANNEL CHECK, ACTUATION DEVICE OPERATIONAL TEST, CALIBRATION, SENSOR OPERATIONAL TEST, EXTENDED SELF TESTS, and RESPONSE TIME testing.

The SRs are modified by a Note. The Note directs the reader to Table 3.3.8-1 to determine the correct SRs to perform for each Function.

SR 3.3.8.1

Performance of the CHANNEL CHECK ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the 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; therefore, it is key in verifying that the instrumentation continues to operate properly between each CALIBRATION.

BASES

SURVEILLANCE REQUIREMENTS (continued)

Agreement criteria are determined by the plant staff, based on a combination of the channel instrument uncertainties, including isolation, indication, and readability. If a channel is outside the criteria, it may be an indication that the sensor or the signal processing equipment has drifted outside its limit. If the channels are within the criteria, it is an indication that the channels are OPERABLE.

The Frequency of 31 days is based on operating experience that demonstrates that channel failure is rare. The CHANNEL CHECK supplements less formal checks of channels during operational use of the displays associated with the LCO required channels.

SR 3.3.8.2

A SENSOR OPERATIONAL TEST (SOT) is performed every 24 months to ensure the devices will perform their intended function when needed. The test is performed in accordance with the Setpoint Control Program. A SOT shall be the injection of a simulated or actual signal into the division as close to the sensor as practicable to verify OPERABILITY of all devices in the division required for division OPERABILITY. The SOT shall include the verification of the accuracy and time constants of the analog input modules.

The SOT may be performed by means of any series of sequential, overlapping, or total steps.

SR 3.3.8.3

A CALIBRATION of each sensor every 24 months ensures that each instrument division is reading accurately and within tolerance. The test is performed in accordance with the Setpoint Control Program. A CALIBRATION shall be the adjustment, as necessary, of the sensor output such that it responds within the necessary range and accuracy to known values of the parameter that the division monitors. The CALIBRATION shall encompass all devices in the division required for sensor OPERABILITY. The CALIBRATION includes provisions for the following:

BASES

SURVEILLANCE REQUIREMENTS (continued)

1. Evaluation of sensor performance to verify that the sensor is functioning as required prior to returning the sensor to service if the as-found sensor calibration setting values are outside their predefined as-found tolerance for the specified calibration settings (e.g., 0, 25, 50, 75, and 100 percent), but conservative with respect to the Allowable Value, and

2. Declaring the sensor immediately inoperable if the sensor cannot be calibrated such that the as-left sensor calibration setting values are within the specified as-left tolerance around the specified calibration settings (e.g., 0, 25, 50, 75, and 100 percent), at the completion of the surveillance.

The CALIBRATION may be performed by means of any series of sequential, overlapping, or total steps.

SR 3.3.8.4

The features of continuous self-monitoring of the Protection System are described in Reference 3. Additional tests, which require the function processor to be inoperable are not normally performed during operation. These EXTENDED SELF TESTS are performed at start-up of a function processor each cycle. The startup sequence is as follows:

– Hardware basic test using the internal diagnosis monitor,
– Start-up self-test of the operating system, and
– Switch over to normal operation after approximately two minutes.

Additional information is provided in Section 2 of Reference 3.

SR 3.3.8.5

SR 3.3.8.5 is the performance of an ACTUATING DEVICE OPERATIONAL TEST (ADOT) every 24 months. The ADOT may be performed by means of any series of sequential, overlapping, or total steps.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.8.6

This surveillance verifies that the NTSPs have been properly loaded into the applicable APUs. The test is performed in accordance with the Setpoint Control Program.

SR 3.3.8.7

This surveillance verifies that the individual division actuation response times are less than or equal to the maximum values assumed in the accident analysis. Response time testing acceptance criteria are included in a document controlled under 10 CFR 50.59. Individual component response times are not modeled in the analyses.

The analyses model the overall or total elapsed time, from the point at which the parameter exceeds the trip setpoint value at the sensor to the point at which the equipment reaches the required functional state (e.g., EDG automatically achieves the required voltage and frequency within the specified time).

For divisions that include dynamic transfer functions (e.g., lag, lead/lag, rate/lag, etc.), the response time test may be performed with the transfer function set to one, with the resulting measured response time compared to the appropriate FSAR response time. Alternately, the response time test can be performed with the time constants set to their nominal value, provided the required response time is analytically calculated assuming the time constants are set at their nominal values. The response time may be measured by a series of overlapping tests such that the entire response time is measured.

----------REVIEWER'S NOTE----------
The following Bases apply to plants that have obtained NRC approval to utilize allocations for selected components based on NRC-approved U.S. EPR-applicable Topical Reports.

[Response time may be verified by actual response time tests in any series of sequential, overlapping or total division measurements, or by the summation of allocated sensor, signal processing and actuation logic response times with actual response time tests on the remainder of the division. Allocations for sensor response times may be obtained from: (1) historical records based on acceptable response time tests (hydraulic,

BASES

SURVEILLANCE REQUIREMENTS (continued)

noise, or power interrupt tests), (2) in place, onsite, or offsite (e.g., vendor) test measurements, or (3) utilizing vendor engineering specifications. NRC-approved U.S. EPR-applicable Topical Report provides the basis and methodology for using allocated sensor response times in the overall verification of the division response time for specific sensors identified in the report. Response time verification for other sensor types must be demonstrated by test.

NRC-approved U.S. EPR-applicable Topical Report (provide reference) provides the basis and methodology for using allocated signal processing and actuation logic response times in the overall verification of the DCS division response time.

The allocations for sensor, signal conditioning, and actuation logic response times must be verified prior to placing the component in operational service and re-verified following maintenance that may adversely affect response time. In general, electrical repair work does not impact response time provided the parts used for repair are of the same type and value. One example where response time could be affected is replacing the sensing assembly of a transmitter.]

As appropriate, each division's response must be verified every 24 months on a STAGGERED TEST BASIS. Testing of the final actuation devices is included in the testing. Response times cannot be determined during plant operation because equipment operation is required to measure response times. Experience has shown that these components usually pass this surveillance when performed at the 24 month Frequency. Therefore, the Frequency was concluded to be acceptable from a reliability standpoint.

REFERENCES

1. FSAR, Section 7.3.

2. FSAR, Chapter 15.

3. ANP-10315P, Revision 1, "U.S. EPR Protection System Surveillance Testing and Teleperm XS Self-Monitoring Technical Report," June 2011

B 3.3 INSTRUMENTATION

B 3.3.9 Engineered Safety Feature (ESF) Control Instrumentation

BASES

BACKGROUND

Refer to B 3.3.1, “Reactor Trip Instrumentation,” for background information on the Distributed Control System. Refer to B 3.3.2, “Engineered Safety Feature Actuation System (ESFAS) Instrumentation,” for background information that is generically applicable to U.S. EPR systems that perform Engineered Safety Feature (ESF) functions.

Normally, there are four divisions of each ESF function, which utilize four divisions of Input & Acquisition Logic and Actuation Logic. The instrumentation normally actuates the Function using a two-out-of-four voting logic. The actuation of the ESF is performed by the Protection System (PS).

The ESF Control Instrumentation does not actuate equipment; it controls the equipment once it is actuated by other ESF functions. The Safety Automation System (SAS) is designed to perform ESF control functions and automated safety-related closed loop control functions once the safety-related process systems have been initiated by the PS. The SAS provides grouped commands execution initiated from the Safety Information and Control System (SICS). The ESF control signals from the SAS are also sent to the priority and actuator control system (PACS). The PACS prioritizes the signals from the PS and SAS and produces an output signal to the execute features. The ESF Control Instrumentation is designed to provide control of the safety-related systems that are needed to reach safe shutdown of the plant.

The SAS consists of these functional units:

– Control Units (CU),
– Monitoring Service Interfaces (MSI),
– Gateways (GW), and
– Service Unit (SU).

Details on these functional units, along with details of the PS architecture, are described in the U.S. EPR Protection System Technical Report (ANP-10309P) (Reference 1).

The CUs execute the logic for the assigned automatic and manual grouped control functions. There are redundant pairs of CUs within a division. Redundant pairs of CUs that perform functions requiring interdivisional communication identified in Reference 2 have data communications between CUs in different divisions or those redundant

BASES

BACKGROUND (continued)

pairs of CUs that do not have any functions allocated that require interdivisional communication, there are no data connections between redundant pairs CUs in different divisions. The CUs acquire hardwired inputs from the signal conditioning and distribution system (SCDS), the PS, or the SICS via hardwired connections. Hardwired outputs from the CUs are sent to the PACS for signal prioritization and drive actuation. Hardwired outputs may also be sent to the Process Automation System (PAS) to coordinate logic for related actuators within PAS.

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

The Distributed Control System (DCS) is designed to ensure that the following operational criteria are met:

– The associated actuation will occur when the parameter monitored by each division reaches its setpoint and the specific coincidence logic is satisfied; and

– In general, separation and redundancy are maintained to permit a division to be out of service for testing or maintenance while still maintaining redundancy within the DCS instrumentation network.

The Conditions address the following groups of components:

– Logic Input Division: The portion of the logic that reads in the plant parameter (e.g. temperature and valve position) and provides the signal to the Control Logic Division. The hardware includes the sensor and conditioning equipment associated with the sensor (e.g. signal conditioning and distribution system), up to the input of the CUs.
– Control Logic Division: The portion of the logic that receives the plant parameter and performs further conditioning (e.g. filters), calculations, comparison of values to setpoints, voting, and sends an actuation signal to PACS. The hardware includes the CU, hardwired logic downstream of the CU, and cabling to the PACS.
– Manual Division: The portion of the logic that provides a manual input to the Control Logic Division (system-level) or PACS (component-level). The hardware includes the manual device (SICS pushbutton) and cabling to the Control Logic Division or PACS.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

The ESF Control Instrumentation supports the following Functions:

1. Emergency Feedwater System (EFWS) Pump Flow Overflow Protection

In case of loss of Main Feedwater, the EFWS is actuated by the PS to remove residual heat via the secondary side. The PS function ensures heat is removed from the primary system through the Steam Generators (SGs) in the event of a loss of MFW or feedwater line break, as indicated by low SG level. EFWS pump overflow protection is designed to limit the flow to a depressurized steam generator to limit overcooling.

This feature is credited for a MSLB and is, therefore, required for Modes 1, 2, and 3. In Mode 4, because of the reactivity inserted by control rods, the reactor would not return to critical even if the RCS temperature was reduced to room temperature.

a. EFWS Pump Flow Overflow Protection - Automatic

Four divisions of the EFWS Pump Flow Overflow Protection – Automatic Function are required to be OPERABLE in MODES 1, 2, and 3.

This Function utilizes the EFW Pump Discharge Flow sensors.

The NTSP is low enough to provide an operating envelope that prevents unnecessary actuations but high enough to ensure sufficient make-up is provided to the SGs.

There are no permissives associated with this Function.

This Function satisfies the requirements of Criterion 3 of 10 CFR 50.36(c)(2)(ii).

b. EFWS Pump Flow Protection - Manual

Four divisions of the EFWS Pump Flow Protection – Manual Function are required to be OPERABLE in MODES 1, 2, and 3.

The capability for manual system-level operation of the EFWS Pump Flow Protection – Manual is provided on the SICS in the MCR. Two divisions of the EFWS Pump Flow

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

Protection – Manual Function are required to be OPERABLE in MODE 4 when the SGs are relied upon for heat removal.

There is no NTSP associated with this Function.

There are no permissives associated with this Function.

This Function satisfies the requirements of Criterion 4 of 10 CFR 50.36(c)(2)(ii).

2. EFWS Level Control

a. EFWS Level Control - Manual

In case of loss of Main Feedwater, the EFWS is actuated by the PS to remove residual heat via the secondary side. The function ensures heat is removed from the primary system through the Steam Generators (SGs) in the event of a loss of MFW or feedwater line break, as indicated by low SG level.

This Function mitigates a Steam Generator Tube Rupture.

Four divisions of this Function are required to be OPERABLE in MODES 1, 2, and 3.

The capability for component-level control of the MHSI Large Miniflow valves is available to the operator on the SICS in the MCR. There are series of switches (i.e., open/close/stop) for each valve.

There is no NTSP associated with this Function.

There are no permissives associated with this Function.

This Function satisfies the requirements of Criterion 4 of 10 CFR 50.36(c)(2)(ii).

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

3. Main Steam Relief Control Valve (MSRCV) Standby Position Control

a. Main Steam Relief Control Valve (MSRCV) Standby Position Control - Automatic

When the MSRIV is not open, the MSRCV is continuously controlled by the SAS based on reactor power. This is a pre-positioning function that allows the MSRCV to be in position when the MSRIV receives a PS signal to open.

Four divisions of this Function are required to be OPERABLE in MODES 1, 2, and 3 and in MODE 4 when the SGs are relied upon for heat removal.

This Function utilizes the following sensors:

– MSRIV Position Indication, and
– SG Pressure.

There is no NTSP associated with this Function.

There are no permissives associated with this Function.

This Function satisfies the requirements of Criterion 3 of 10 CFR 50.36(c)(2)(ii).

4. MSRCV Pressure Control

a. MSRCV Pressure Control - Automatic

Whenever the Main Steam Relief Isolation Valve is opened by the PS, the MSRCV is modulated by the SAS to maintain SG pressure at the Max1p setpoint. This control uses the difference between measured SG pressure and the Max1p value to determine the MSRCV position.

Four divisions of this Function are required to be OPERABLE in MODES 1, 2, and 3.

This function utilizes the following sensors:

– MSRIV Position Indication, and
– SG Pressure.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

There is no NTSP associated with this Function.

There are no permissives associated with this Function.

This Function satisfies the requirements of Criterion 3 of 10 CFR 50.36(c)(2)(ii).

b. MSRCV Pressure Control - Manual

The capability for manual system-level opening of the MSRIV on a per-train basis is provided

Four divisions of this Function are required to be OPERABLE in MODES 1, 2, and 3 and in MODE 4 when the SGs are relied upon for heat removal.

The capability for manual system-level opening of the MSRIV on a per-train basis is provided on the SICS in the MCR. Two manual system-level initiation controls are provided per MSRIV. Any one of these two controls opens the desired MSRIV.

There is no NTSP associated with this Function.

There are no permissives associated with this Function.

This Function satisfies the requirements of Criterion 4 of 10 CFR 50.36(c)(2)(ii).

5. Control Logic

Four divisions of this Function are required to be OPERABLE in MODES 1, 2, and 3 and in MODE 4 when the SGs are relied upon for heat removal.

This Function satisfies the requirements of Criterion 3 of 10 CFR 50.36(c)(2)(ii).

BASES

ACTIONS

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

A.1

Condition A applies to all ESF Control Instrumentation Functions. Condition A addresses the situation where one or more Functions with one or more required divisions are inoperable. The Required Action is to refer to Table 3.3.9-1 and to take the Required Actions for the Functions affected. The Completion Times are those from the referenced Conditions and Required Actions.

B.1

Condition B applies to the EFWS Pump Flow Overflow Protection – Logic Input Division. Condition A addresses the situation where one or more divisions are inoperable. The Required Action is to immediately enter the applicable Conditions and Required Actions of LCO 3.7.5, "Emergency Feedwater (EFW) System" for division(s) made inoperable by the ESF Control Instrumentation. The purpose of each referenced action is addressed in the Bases for these sections. The Completion Time of immediately is consistent with the required times for actions requiring prompt attention.

C.1

Condition C applies when one or more Main Steam Relief Control Valve (MSRCV) Standby Position Control – Automatic or MSRCV Pressure Control – Logic Input divisions are inoperable.

The Required Action is to immediately enter the applicable Conditions and Required Actions of LCO 3.7.4, "Main Steam Relief Trains (MSRT)" for valve(s) made inoperable by the ESF Control Instrumentation. The purpose of each referenced action is addressed in the Bases for these sections. The Completion Time of immediately is consistent with the required times for actions requiring prompt attention.

BASES

ACTIONS (continued)

D.1 and D.2

Condition D applies when one or more Manual or Control Logic divisions are inoperable.

Required Action D.1 is modified by a Note indicating this Condition is only applicable to the following Functions:

1. b, EFWS Pump Flow Overflow Protection - Manual,
2. EFWS Level Control - Manual, and
5. Control Logic.

The Required Action is to immediately enter the applicable Conditions and Required Actions of LCO 3.7.5, "Emergency Feedwater (EFW) System" for division(s) made inoperable by the ESF Control Instrumentation. The purpose of each referenced action is addressed in the Bases for these sections. The Completion Time of immediately is consistent with the required times for actions requiring prompt attention.

Required Action D.2 is modified by a Note indicating this Condition is only applicable to the following Functions:

4.b. MSRCV Pressure Control - Manual, and
5. Control Logic.

The Required Action is to immediately enter the applicable Conditions and Required Actions of LCO 3.7.4, "Main Steam Relief Trains (MSRT)" for valve(s) made inoperable by the ESF Control Instrumentation. The purpose of each referenced action is addressed in the Bases for these sections. The Completion Time of immediately is consistent with the required times for actions requiring prompt attention.

E.1 and E.2

Condition E applies when one or more Logic Input divisions, Manual divisions, or Control Logic divisions cannot be restored to OPERABLE status in the time allowed by Required Actions B.1, C.1, D.1, or D.2. The plant must be brought to a MODE where the LCO is no longer applicable.

The Completion Time of 6 hours to reach MODE 3 and 36 hours to reach MODE 5 is reasonable, based on operating experience, to reach the required MODES from full power conditions in an orderly manner and without challenging plant systems.

BASES

ACTIONS (continued)

F.1

Condition F addresses the failure of one required EFWS Pump Flow Overflow Protection – Manual Function divisions in MODE 4. The inoperable Manual division must be restored to OPERABLE status within 72 hours. The Completion Time of 72 hours is reasonable considering that there is one Manual division available, the low probability of an event occurring during this interval, and the time necessary for repairs.

G.1

Condition G addresses the failure of both required EFWS Pump Flow Overflow Protection – Manual Function divisions or the inability to complete the remedial measures in the time allowed by Required Action F.1. The plant must be brought to a MODE where the LCO is no longer applicable. To achieve this status, the plant must be brought to MODE 4 without reliance upon steam generator for heat removal. The Completion Time of 24 hours to reach MODE 4 without reliance upon a steam generator for heat removal is reasonable, based on operating experience, to reach the required power level from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

The SRs for each Function are identified by the Surveillance Requirements (SR) column of Table 3.3.9-1 for that Function. Most Functions are subject to CHANNEL CHECK, ACTUATION DEVICE OPERATIONAL TEST, CALIBRATION, SENSOR OPERATIONAL TEST, and EXTENDED SELF TESTS.

The SRs are modified by a Note. The Note directs the reader to Table 3.3.1-9 to determine the correct SRs to perform for each Function.

SR 3.3.9.1

Performance of the CHANNEL CHECK ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the 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

BASES

SURVEILLANCE REQUIREMENTS (continued)

CHECK will detect gross channel failure; therefore, it is key in verifying that the instrumentation continues to operate properly between each CALIBRATION.

Agreement criteria are determined by the plant staff, based on a combination of the channel instrument uncertainties, including isolation, indication, and readability. If a channel is outside the criteria, it may be an indication that the sensor or the signal processing equipment has drifted outside its limit. If the channels are within the criteria, it is an indication that the channels are OPERABLE.

The Frequency of 31 days is based on operating experience that demonstrates that channel failure is rare. The CHANNEL CHECK supplements less formal checks of channels during operational use of the displays associated with the LCO required channels.

SR 3.3.9.2

A SENSOR OPERATIONAL TEST (SOT) is performed every 24 months to ensure the devices will perform their intended function when needed. A SOT shall be the injection of a simulated or actual signal into the division as close to the sensor as practicable to verify OPERABILITY of all devices in the division required for division OPERABILITY. The SOT shall include the verification of the accuracy and time constants of the analog input modules.

The SOT may be performed by means of any series of sequential, overlapping, or total steps.

SR 3.3.9.3

A CALIBRATION of each sensor every 24 months ensures that each instrument division is reading accurately and within tolerance. A CALIBRATION shall be the adjustment, as necessary, of the sensor output such that it responds within the necessary range and accuracy to known values of the parameter that the division monitors. The CALIBRATION shall encompass all devices in the division required for sensor OPERABILITY.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The CALIBRATION includes provisions for the following:

1. Evaluation of sensor performance to verify that the sensor is functioning as required prior to returning the sensor to service if the as-found sensor calibration setting values are outside their predefined as-found tolerance for the specified calibration settings (e.g., 0, 25, 50, 75, and 100 percent), but conservative with respect to the Allowable Value, and

2. Declaring the sensor immediately inoperable if the sensor cannot be calibrated such that the as-left sensor calibration setting values are within the specified as-left tolerance around the specified calibration settings (e.g., 0, 25, 50, 75, and 100 percent), at the completion of the surveillance.

The CALIBRATION may be performed by means of any series of sequential, overlapping, or total steps.

SR 3.3.9.4

The features of continuous self-monitoring of the SAS are described in Reference 3. Additional tests, which require the function processor to be inoperable are not normally performed during operation. These EXTENDED SELF TESTS are performed at start-up of a function processor each cycle. The startup sequence is as follows:

– Hardware basic test using the internal diagnosis monitor,
– Start-up self-test of the operating system, and
– Switch over to normal operation after approximately two minutes.

Additional information is provided in Section 2 of Reference 3.

SR 3.3.9.5

SR 3.3.9.5 is the performance of an ADOT every 31 days. This test shall verify OPERABILITY by actuation of the RTBs and RTCs. The ADOT may be performed by means of any series of sequential, overlapping, or total steps.

BASES

REFERENCES

1. ANP-10309P, Revision 4, “U.S. EPR Protection System Technical Report,” AREVA NP Inc., May 2012.

2. FSAR, Section 7.1.

3. ANP-10315, Revision 2, “U.S. EPR Surveillance Testing and TELEPERM XS Self-Monitoring Technical Report.”]

B 3.3 INSTRUMENTATION

B 3.3.10 Engineered Auxiliary Support (EAS) Control Instrumentation

BASES

BACKGROUND

Refer to B 3.3.1, “Reactor Trip Instrumentation,” for background information on the Distributed Control System. Refer to B 3.3.2, “Engineered Safety Feature Actuation System (ESFAS) Instrumentation,” for background information that is generically applicable to U.S. EPR systems that perform Engineered Safety Feature (ESF) functions.

Normally, there are four divisions of each ESF function, which utilize four divisions of Input & Acquisition Logic and Actuation Logic. The instrumentation normally actuates the Function using a two-out-of-four voting logic. The actuation of the ESF is performed by the Protection System (PS).

The ESF Control Instrumentation does not actuate equipment; it controls the equipment once it is actuated by other ESF functions. Control functions are not associated with a Nominal Trip Setpoint since actuation at a specific point is not assumed in the safety analysis.

The safety automation system (SAS) performs closed loop automatic controls of certain ESF systems following their actuation by the PS. The SAS also performs functions for essential auxiliary support (EAS) systems. These are systems that provide support to the ESF systems. The SAS provides grouped commands execution initiated from the Safety Information and Control System (SICS). The ESF control signals from the SAS are also sent to the priority and actuator control system (PACS). The PACS prioritizes the signals from the PS and SAS and produces an output signal to the execute features. The ESF Control Instrumentation is designed to provide control of the safety-related systems that are needed to reach safe shutdown of the plant.

The SAS consists of these functional units:

– Control Units (CU),
– Monitoring Service Interfaces (MSI),
– Gateways (GW), and
– Service Unit (SU).

Details on these functional units, along with details of the PS architecture, are described in the U.S. EPR Protection System Technical Report (ANP-10309P) (Reference 1).

BASES

BACKGROUND (continued)

The CUs execute the logic for the assigned automatic and manual grouped control functions. There are redundant pairs of CUs within a division. Redundant pairs of CUs that perform functions requiring interdivisional communication identified in Reference 2 have data communications between CUs in different divisions or those redundant pairs of CUs that do not have any functions allocated that require interdivisional communication, there are no data connections between redundant pairs CUs in different divisions. The CUs acquire hardwired inputs from the signal conditioning and distribution system (SCDS), the PS, or the SICS via hardwired connections. Hardwired outputs from the CUs are sent to the PACS for signal prioritization and drive actuation. Hardwired outputs may also be sent to the Process Automation System (PAS) to coordinate logic for related actuators within PAS. There are no permissives associated with the EAS Control Instrumentation.

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

The Distributed Control System (DCS) is designed to ensure that the following operational criteria are met:

– The associated actuation will occur when the parameter monitored by each division reaches its setpoint and the specific coincidence logic is satisfied; and
– In general, separation and redundancy are maintained to permit a division to be out of service for testing or maintenance while still maintaining redundancy within the DCS instrumentation network.

The Conditions address the following groups of components:

– Logic Input Division: The portion of the logic that reads in the plant parameter (e.g. temperature and valve position) and provides the signal to the Control Logic Division. The hardware includes the sensor and conditioning equipment associated with the sensor (e.g. signal conditioning and distribution system), up to the input of the CUs.
– Control Logic Division: The portion of the logic that receives the plant parameter and performs further conditioning (e.g. filters), calculations, comparison of values to setpoints, voting, and sends an actuation signal to PACS. The hardware includes the CU, hardwired logic downstream of the CU, and cabling to the PACS.
– Manual Division: The portion of the logic that provides a manual input to the Control Logic Division (system-level) or PACS (component-level). The hardware includes the manual device (SICS pushbutton) and cabling to the Control Logic Division or PACS.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

The EAS Control Instrumentation supports the following Functions:

1. Annulus Ventilation System (AVS)

The AVS maintains a negative pressure in the annulus between the shield building and the Containment Building during operation. Filters in the system control the release of radioactive contaminants to the environment. The AVS design basis is to mitigate the consequences of the limiting Design Basis Accident (DBA), which is a loss of coolant accident (LOCA). Therefore, this Function is required for MODES 1, 2, 3, and 4.

This Function satisfies the requirements of Criterion 3 of 10 CFR 50.36(c)(2)(ii).

a. AVS - Accident Filtration Train Heater Control

The AVS has a safety-related function to maintain capability of the iodine absorbers to remove iodine from the annulus exhaust air. The heaters are used to limit the relative humidity to a maximum of 70 percent in order to maintain the capability of the iodine absorbers to remove iodine from the annulus exhaust air when the AVS accident trains are in operation.

This Function utilizes two Temperature, a Heater Fan Running, and two Isolation Damper Open sensors per division.

b. AVS - Accident Train Isolation on Containment Isolation

The AVS has a safety-related function to maintain a negative pressure and provide exhaust filtration. In case of a failure during accident operation of an operating accident filtration train, and a negative pressure is not being maintained in the annulus, operation is switched to the non-operating accident filtration train to maintain a negative pressure and provide exhaust filtration.

The sensors utilized to initiate containment isolation for the containment isolation Functions are described in the Bases for LCO 3.3.4, “Containment Isolation Instrumentation.”

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

2. Component Cooling Water System (CCWS)

The CCWS is a closed loop cooling water system that, in conjunction with the essential service water system (ESWS) and the ultimate heat sink (UHS), removes heat generated from the plant's safety related components connected to the CCWS during an anticipated operational occurrence (AOO) or postulated accident. During normal operation, the CCW System also provides this function for various nonessential components, as well as the spent fuel storage pool. The CCW System serves as a barrier to the release of radioactive byproducts between potentially radioactive systems and the ESWS and thus to the environment. Therefore, this Function is required for MODES 1, 2, 3, and 4.

This Function satisfies the requirements of Criterion 3 of 10 CFR 50.36(c)(2)(ii).

a. CCW System - Common Header 1.b and 2.b Automatic Backup Switchover

The safety-related function to perform an automatic switchover from Train 1 to Train 2 verifies that the CCWS is capable of fulfilling its safety-related function to remove heat from safety-related components on the CCWS Common 1.a and 1.b headers.

This Function utilizes a Loss of ESWS, Pump Discharge Pressure, and Flow Rate sensor in each division.

b. CCW System - Emergency Temperature Control

The safety-related function to control the CCWS heat exchanger outlet temperature is required to maintain the temperature of the cooling water within its limits. This verifies that the CCWS is capable of fulfilling its safety-related function to remove heat from safety-related components.

This Function utilizes three Heat Exchanger Temperature sensors and a Heat Exchanger Bypass Valve Closed sensor in each division.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

c. CCW System - Emergency Leak Detection

The safety-related function for emergency leak detection maintains the required cooling water inventory that supports the safety-related function to remove heat using indications to detect leaks and isolate them.

This Function utilizes the following sensors in each division:

– Two Surge Tank Level,
– One OCWS Chiller Inlet Flow,
– One OCWS Chiller Outlet Flow,
– One Non-Safety Common Users Outlet Flow, and
– One Non-Safety Common Users Inlet Flow.

d. CCW System - Emergency Leak Detection - Switchover Valves Leakage or Failure

The safety-related function for switchover valve leakage or failure isolates the CCW System trains from their common headers so that each train is able to provide their corresponding Low Head Safety Injection heat exchanger with the required flow for heat removal.

This Function utilizes two Surge Tank Level sensors in each division.

e. CCW System - Switchover Valves Interlock

Interlocks are provided so that no two redundant CCWS trains are connected to the same common header at the same time.

This Function utilizes the following sensors:

– Four Train 1 Common 1a Supply Closed,
– Four Train 1 Common 1b Supply Closed,
– Four Train 2 Common 1a Supply Closed,
– Four Train 2 Common 1b Supply Closed,
– Four Train 3 Common 1a Supply Closed,
– Four Train 3 Common 1b Supply Closed,
– Four Train 4 Common 1a Supply Closed, and
– Four Train 4 Common 1b Supply Closed.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

f. CCW System - Reactor Coolant Pump (RCP) Thermal Barrier Containment Isolation Valves Interlock

An interlocking function is required for the cooling paths of the Common 1b and Common 2b headers for the reactor coolant pump (RCP) thermal barriers. Either the Common 1b or 2b header can provide cooling to the RCP thermal barriers. To maintain strict CCWS train separation, one of the supply containment isolation valves (CIV) and one of the return CIVs on the RCP thermal barriers cooling path must be closed on the header being removed from service (1b or 2b) prior to opening the CIVs on the header being placed in service (2b or 1b, respectively).

This Function utilizes the following sensors:

– Two Common 1b Supply Inner Containment Isolation Valve Closed,
– Two Common 1b Return Inner Containment Isolation Valve Closed,
– Two Common 1b Supply Outer Containment Isolation Valve Closed,
– Two Common 1b Return Outer Containment Isolation Valve Closed,
– Two Common 2b Supply Inner Containment Isolation Valve Closed,
– Two Common 2b Return Inner Containment Isolation Valve Closed,
– Two Common 2b Supply Outer Containment Isolation Valve Closed, and
– Two Common 2b Return Outer Containment Isolation Valve Closed.

g. CCW System - RCP Thermal Barrier Containment Isolation Valves Opening Interlock

An interlock function is required to open the CIVs on the common header removed from service (1b or 2b) when a CIV on the common header in service (2b or 1b, respectively) is closed.

This Function utilizes the following sensors:

– Two Common 1b Supply Inner Containment Isolation Valve Closed,
– Two Common 1b Return Inner Containment Isolation Valve Closed,
– Two Common 1b Supply Outer Containment Isolation Valve Closed,
– Two Common 1b Return Outer Containment Isolation Valve Closed,
– Two Common 2b Supply Inner Containment Isolation Valve Closed,
– Two Common 2b Return Inner Containment Isolation Valve Closed,
– Two Common 2b Supply Outer Containment Isolation Valve Closed, and
– Two Common 2b Return Outer Containment Isolation Valve Closed.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

h. CCW System - Safety Chilled Water System Condenser Supply Water Flow Control

The CCWS has a safety-related function that controls CCWS flow to the SCWS condenser and provides a heat sink for heat rejection,

This Function utilizes the Condenser Refrigerant Pressure sensors.

3. Essential Service Water System (ESWS) Pump Building Ventilation System

a. ESWS Pump Building Ventilation System - ESWS Pump Rooms Temperature Control

The essential service water pump building ventilation system has a safety related function that maintains the ESWS pump room temperature when the ESWS pumps are operating at rated load and the outside air is at maximum site design ambient temperature.

Therefore, this Function is required for MODES 1, 2, 3, and 4.

This Function satisfies the requirements of Criterion 3 of 10 CFR 50.36(c)(2)(ii).

This Function utilizes an Outside Air Temperature sensor in each division.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

4. Fuel Building Ventilation System (FBVS)

The FBVS maintains acceptable ambient conditions in the fuel building to permit personnel access and to control airborne radioactivity in the area during normal plant operation, anticipated occurrences, and following fuel handling accidents.

This Function satisfies the requirements of Criterion 3 of 10 CFR 50.36(c)(2)(ii).

a. FBVS - Extra Borating System (EBS) Heater Control

The FBVS has a safety-related function that maintains the temperature in the boron rooms and surrounding extra borating system tanks to prevent crystallization in extra borating system piping.

The EBS is required to be OPERABLE in MODES 1, 2, 3, 4, and 5. Therefore, this support Function is also required for MODES 1, 2, 3, 4, and 5.

This Function utilizes two EBS Room Temperature and two Pipe Chase Room Temperature sensors per division in Divisions 1 and 4.

b. FBVS - EBS Pump Room Heat Removal

The FBVS has a safety-related function that maintains the room ambient conditions in the extra borating system pump rooms and fuel pool cooling system pump rooms.

The EBS is required to be OPERABLE in MODES 1, 2, 3, 4, and 5. Therefore, this support Function is also required for MODES 1, 2, 3, 4, and 5.

This Function utilizes two Fuel Pool Cooling and Purification System Pump Room Temperature sensors and one EBS Pump Room temperature sensor per division in Divisions 1 and 4.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

5. Main Control Room (MCR) Air Conditioning System

The main control room air conditioning system (CRACS) is designed to maintain design temperature and conditions for rooms within the Control Room Envelope (CRE) during normal and accident conditions. Therefore, this Function is required for MODES 1, 2, 3, 4, 5, and 6 and during movement of irradiated fuel assemblies.

This Function satisfies the requirements of Criterion 3 of 10 CFR 50.36(c)(2)(ii).

a. Control Room Emergency Filtration (CREF) Iodine Filtration Train Heater Control

The CRACS has a safety-related function to preheat the inlet air in order to reduce the airborne moisture prior to entry into the carbon bed within the filter unit. The relative humidity is limited to a maximum of 70% in order to maintain the capability of the carbon filters to remove iodine from the annulus supply air.

This Function utilizes a Protective Switch Off Temperature, two Carbon Filter Isolation Damper Position, and a ESF Filtration Booster Fan Not Running sensor per division in Divisions 1 and 4.

b. CREF Heater Control for Outside Inlet Air

The CRACS has a safety-related function to preheat the outside air. The heaters are designed to heat the outside air during cold weather conditions and to preheat the cold outside air to prevent the CRACS air handling unit chilled water cooling coils from freezing.

This Function utilizes two Downstream of Electric Heater Temperature, one Inlet Damper Open, and one Outlet Damper Open sensors per division in Divisions 1 and 4.

c. CRACS Pressure Control

The CRACS has a safety-related function to verify the MCR is maintained at a positive pressure with respect to the ambient air pressure in adjacent areas to prevent unfiltered in-leakage into the MCR and associated rooms.

This Function utilizes a MCR and Reference Room Differential Pressure sensor in Divisions 1 and 4.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

d. CRACS Cooler Temperature Control

The CRACS has safety-related functions that verify that the air supply temperature is maintained within the preset temperature range.

This Function utilizes a Supply Air Temperature sensor in each division.

6. Safeguards Building Controlled Area Ventilation System (SBVS)

The SBVS provides a suitable and controlled environment, in the mechanical areas of the safeguard buildings where ESF components are located, for personnel access and to allow safe operation of the equipment during normal plant operation, outages and under AOOs and PAs. Therefore, this Function is required for MODES 1, 2, 3, and 4.

This Function satisfies the requirements of Criterion 3 of 10 CFR 50.36(c)(2)(ii).

a. SBVS - Safety Injection System (SIS) / Residual Heat Removal System (RHRS) Pump Room Heat Removal

The SBVS has a safety-related function that maintains ambient conditions below the maximum limits for the rooms of the SIS / RHRS safety-related system components.

This Function utilizes the following sensors in each division:

– Two MHSI Pump Room Temperature,
– Two Low Head Safety Injection (LHSI) Pump Room Temperature,
– One SIS/RHR Pump Running, and
– One SIS/RHR Pump Stopped.

b. SBVS - CCWS / Emergency Feedwater System (EFWS) Valve Rooms Heat Removal

The SBVS has a safety-related function that maintains ambient conditions below the maximum limits for the rooms of the CCWS/EFWS safety-related system components.

This Function utilizes two Room Temperature sensors in each division.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

c. SBVS - Safeguards Building HVAC Reconfiguration on Containment Isolation

The SBVS has a safety-related function to automatically isolate the Safeguard Building hot mechanical areas and initiate filtration of exhaust from the areas in the event of a containment isolation signal.

The sensors utilized to initiate containment isolation for the containment isolation Functions are described in the Bases for LCO 3.3.4, "Containment Isolation Instrumentation."

d. SBVS - Fuel Building Isolation on Containment Isolation

The Fuel Building Ventilation System has a safety-related function to automatically isolate the supply and exhaust ducts in the event of a containment isolation signal.

The sensors utilized to initiate containment isolation for the containment isolation Functions are described in the Bases for LCO 3.3.4, "Containment Isolation Instrumentation."

7. Safeguards Building Ventilation System Electrical Division (SBVSE)

The SBVSE maintains acceptable ambient conditions for the safety related electrical equipment, EFW pump rooms and CCWS component rooms in the Safeguard Building during normal plant operation and accident conditions. Therefore, this Function is required for MODES 1, 2, 3, and 4.

This Function satisfies the requirements of Criterion 3 of 10 CFR 50.36(c)(2)(ii).

a. SBVSE - Supply and Recirculation-Exhaust Air Flow Control

The SBVSE has a safety-related function to control supply, exhaust, and recirculation air flow as required to maintain ambient temperature and air quality (via filtration) within applicable limits for safety-related equipment located within the Safeguard Building areas and rooms.

This Function utilizes the following sensors in each division:

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

– Two Supply Air Downstream of Heaters Temperature,
– Protective Switch-off Temperature,
– Two Outside Are Temperature,
– Outside Air Damper Position Open,
– Outside Air Damper Position Close,
– Exhaust Damper Position Open,
– Exhaust Damper Position Close,
– Recirculation Damper Position Open, and
– Recirculation Damper Position Close.

b. SBVSE - Supply Fan Safe Shut-Off

An inadvertent stopping of the supply fan, due to a spurious system action, may cause the SBVSE for a given division to become inoperable. Therefore, to mitigate the risk of system spurious actions, this function is to be designated as safety-related.

This Function utilizes the following sensors in each division:

Recirculation /Exhaust Air Fan Motor Stopped,
Outside Air Damper Position Closed, and
Recirculation Damper Position Closed.

c. SBVSE - Recirculation Fan Safe Shut-Off

An inadvertent stopping of the recirculation/exhaust fan, due to a spurious system action, may cause the SBVSE for a given division to become inoperable. Therefore, to mitigate the risk of system spurious actions, this function is to be designated as safety-related.

This Function utilizes two Component Cooling Water Pump Room Temperature and two Emergency Feedwater Pump Room Temperature sensors in each division.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

d. SBVSE - Exhaust Fan Safe Shut-off

An inadvertent stopping of the exhaust fan, due to a spurious system action, may cause the SBVSE for a given division to become inoperable. Therefore, to mitigate the risk of system spurious actions, this function is to be designated as safety-related.

This Function utilizes an Exhaust Damper Position Closed sensor in each division.

e. SBVSE - Supply Air Temperature Heater Control

The SBVSE has a safety-related function to maintain supply air temperature (downstream of heaters) as required to maintain ambient temperature within applicable limits for safety-related equipment located within the Safeguard Building areas and rooms.

This Function utilizes a Filter Bank Differential Pressure and two Supply Air Downstream of Heaters Temperature sensors in each division.

f. SBVSE - Supply Air Temperature Control for Supply Air Cooling

The SBVSE has a safety-related function to maintain a constant air temperature, as required, to maintain ambient temperature within applicable limits for safety-related equipment located within the Safeguard Building areas and rooms.

This Function utilizes a Supply Air Downstream of Humidifier Temperature sensor in each division.

g. SBVSE - Battery Room heater Control

The SBVSE has a safety-related function to maintain battery room ambient temperature within applicable limits.

This Function utilizes two Supply Air Downstream of Heaters Flow and two Battery Room Temperature sensors in Divisions 1 and 4 and one Supply Air Downstream of Heaters Flow and one Battery Room Temperature sensor in Divisions 2 and 3.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

h. SBVSE - Battery Room Supply Air Temperature Control

The SBVSE has a safety-related function to maintain battery room ambient temperature within applicable limits.

This Function utilizes two Supply Air to Battery Room Temperature sensors each in Divisions 1 and 4 and one Supply Air to Battery Room Temperature sensor each in Divisions 2 and 3.

i. SBVSE - Emergency Feedwater System (EFWS) Pump Room Heat Removal

The SBVSE has a safety-related function to remove heat from the pump room and maintain room temperature within a temperature band for safety-related equipment.

This Function utilizes two Pump Room Temperature sensors in each division.

j. SBVSE - Component Cooling Water System (CCWS) Pump Room Heat Removal

The SBVSE has a safety-related function to remove heat from the applicable rooms and maintain room temperature within a temperature band for safety-related equipment.

This Function utilizes two Pump Room Temperature sensors in each division.

8. Safety Chilled Water System (SCWS)

a. SCWS - SCWS Train Switchover on Low Evaporator Flow / Chiller Blackbox Internal Fault / SCWS Chiller Evaporator Water Flow Control / LOOP Re-Start Failure Interlock

These safety-related automatic switchover functions provide that during a failure that prevents the train in service from transferring heat loads, the redundant train turns on to transfer the heat loads from the safety-related SSC.

The SCWS Train 1 to Train 2 Switchover on Train 1 Lower Evaporator Flow / Chiller Blackbox Internal Fault / SCWS Chiller Evaporator Water Flow Control / LOOP Re-Start Failure Interlock Function utilizes the following sensors:

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

– Train 1 Chiller Evaporator Outlet Temperature,
– Train 1 Chiller Compressor Oil Pressure,
– Train 1 Condenser Refrigerant Pressure,
– Train 1 Chiller Evaporator Flow,
– Two Train 1 Cross-Tie Valves Position Open,
– Two Train 2 Cross-Tie Valves Position Open,
– Train 2 Circulating Pump 1 Running,
– Train 2 Circulating Pump 2 Running,
– Evaporator Delta-Pressure Measurement, and
– Train 2 Chiller Evaporator Flow.

The SCWS Train 2 to Train 1 Switchover on Train 2 Low Evaporator Flow / Chiller Blackbox Internal Fault / Loss of UHS-CCWS / SCWS Chiller Evaporator Water Flow Control / LOOP Re-Start Failure Interlock Function utilizes the following sensors:

– Train 1 Chiller Evaporator Flow,
– Train 1 Circulating Pump 1 Running,
– Train 1 Circulating Pump 2 Running,
– Train 2 Chiller Evaporator Outlet Temperature,
– Train 2 Condenser Flow Rate,
– Train 2 Condenser Refrigerant Pressure,
– Two Train 1 Cross-Tie Valves Position Open,
– Two Train 2 Cross-Tie Valves Position Open,
– Evaporator Delta-Pressure Measurement, and
– Train 2 Chiller Evaporator Flow.

The SCWS Train 3 to Train 4 Switchover on Train 3 Low Evaporator Flow / Chiller Blackbox Internal Fault / Loss of UHS-CCWS / SCWS Chiller Evaporator Water Flow Control / LOOP Re-Start Failure Interlock utilizes the following sensors:

– Train 3 Condenser Flow Rate,
– Train 3 Chiller Evaporator Outlet Temperature,
– Train 3 Chiller Compressor Oil Pressure,
– Train 3 Condenser Refrigerant Pressure,
– Train 3 Chiller Evaporator Flow,
– Two Train 3 Cross-Tie Valves Position Open,
– Two Train 4 Cross-Tie Valves Position Open,
– Train 4 Circulating Pump 1 Running,
– Train 4 Circulating Pump 2 Running,
– Evaporator Delta-Pressure Measurement, and
– Train 4 Chiller Evaporator Flow.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

The SCWS Train 4 to Train 3 Switchover on Train 4 Low Evaporator Flow / Chiller Blackbox Internal Fault / SCWS Chiller Evaporator Water Flow Control / LOOP Re-Start Failure Interlock Function utilizes the following sensors:

– Train 3 Chiller Evaporator Flow,
– Train 3 Circulating Pump 1 Running,
– Train 3 Circulating Pump 2 Running,
– Evaporator Delta-Pressure Measurement,
– Two Train 3 Cross-Tie Valves Position Open,
– Two Train 4 Cross-Tie Valves Position Open,
– Train 4 Chiller Evaporator Flow,
– Train 4 Condenser Refrigerant Pressure,
– Train 4 Chiller Compressor Oil Pressure, and
– Train 4 Chiller Evaporator Outlet Temperature,

9. Safety Injection / Residual Heat Removal (RHR) System

a. RHR Shutdown Valve Interlock

In RHR mode, each Low Head Safety Injection (LHSI) train takes suction from its respective hot leg through two motor operated isolation valves in series (first and second RHR reactor coolant pressure boundary (RCPB) isolation valves). These isolation valves are interlocked to prevent their opening when RCS pressure and temperature have not decreased below acceptable values. These acceptable values are the P14 permissive pressure and temperature thresholds.

This Function utilizes the following sensors:

– Eight Train 1 LHSI Suction Isolation Valve Closed,
– Train 1 RHR First Reactor Coolant Pressure Boundary (RCPB) Isolation Valve Open,
– Train 2 RHR Second RCPB Isolation Valve Open,
– Train 2 RHR First RCPB Isolation Valve Open,
– Train 1 RHR Second RCPB Isolation Valve Open,
– Train 3 RHR First RCPB Isolation Valve Open,
– Train 4 RHR Second RCPB Isolation Valve Open,
– Train 4 RHR First RCPB Isolation Valve Open, and
– Train 3 RHR Second RCPB Isolation Valve Open.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

10. Control Logic

Four divisions of this Function are required to be OPERABLE in MODES 1, 2, 3, and 4. Three divisions of this Function are required to be OPERABLE in MODES 5 and 6 and when irradiated fuel is being moved.

ACTIONS

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

A.1

Condition A applies to all EAS Control Instrumentation Functions. Condition A addresses the situation where one or more Functions with one or more required divisions are inoperable. The Required Action is to refer to Table 3.3.10-1 and to take the Required Actions for the Functions affected. The Completion Times are those from the referenced Conditions and Required Actions.

B.1

Condition B applies when one or more Input or Control Logic divisions are inoperable. The Required Action is to immediately enter the applicable Conditions and Required Actions of LCO 3.6.7, "Annulus Ventilation System (AVS)," for division(s) made inoperable by the EAS Control Instrumentation. The purpose of each referenced action is addressed in the Bases for these sections. The Completion Time of immediately is consistent with the required times for actions requiring prompt attention.

C.1

Condition C applies when one or more Logic Input or Control Logic divisions are inoperable. The Required Action is to immediately enter the applicable Conditions and Required Actions of LCO 3.7.7, "Component Cooling Water (CCW) System," for division(s) made inoperable by the EAS Control Instrumentation. The purpose of each referenced action is addressed in the Bases for these sections. The Completion Time of immediately is consistent with the required times for actions requiring prompt attention.

BASES

ACTIONS (continued)

D.1

Condition D applies when one or more Logic Input or Control Logic divisions are inoperable. The Required Action is to immediately enter the applicable Conditions and Required Actions of LCO 3.7.8, "Essential Service Water (ECW) System," for division(s) made inoperable by the EAS Control Instrumentation. The purpose of each referenced action is addressed in the Bases for these sections. The Completion Time of immediately is consistent with the required times for actions requiring prompt attention.

E.1

Condition E applies when one or more Logic Input or Control Logic divisions are inoperable. The Required Action is to immediately enter the applicable Conditions and Required Actions of LCO 3.5.5, "Extra Borating System (EBS)," for division(s) made inoperable by the EAS Control Instrumentation. The purpose of each referenced action is addressed in the Bases for these sections. The Completion Time of immediately is consistent with the required times for actions requiring prompt attention.

F.1

Condition F applies when one or more Logic Input or Control Logic divisions are inoperable. The Required Action is to immediately enter the applicable Conditions and Required Actions of LCO 3.7.10, "Control Room Emergency Filtration (CREF)," for division(s) made inoperable by the EAS Control Instrumentation. The purpose of each referenced action is addressed in the Bases for these sections. The Completion Time of immediately is consistent with the required times for actions requiring prompt attention.

G.1

Condition G applies when one or more Logic Input or Control Logic divisions are inoperable. The Required Action is to immediately enter the applicable Conditions and Required Actions of LCO 3.7.11, "Control Room Air Conditioning System (CRACS)," for division(s) made inoperable by the EAS Control Instrumentation. The purpose of each referenced action is addressed in the Bases for these sections. The Completion Time of immediately is consistent with the required times for actions requiring prompt attention.

BASES

ACTIONS (continued)

H.1

Condition H applies when one or more Logic Input or Control Logic divisions are inoperable. The Required Action is to immediately enter the applicable Conditions and Required Actions of LCO 3.5.2, "ECCS - Operating," and LCO 3.5.3, "ECCS - Shutdown, MODE 4"," for division(s) made inoperable by the EAS Control Instrumentation. The purpose of each referenced action is addressed in the Bases for these sections. The Completion Time of immediately is consistent with the required times for actions requiring prompt attention.

I.1

Condition I applies when one or more Logic Input or Control Logic divisions are inoperable. The Required Action is to immediately enter the applicable Conditions and Required Actions of LCO 3.7.13, "Safeguard Building Ventilation System Electrical Division (SBVSED)" for division(s) made inoperable by the EAS Control Instrumentation. The purpose of each referenced action is addressed in the Bases for these sections. The Completion Time of immediately is consistent with the required times for actions requiring prompt attention.

J.1

Condition J applies when one or more Logic Input or Control Logic divisions are inoperable. The Required Action is to immediately enter the applicable Conditions and Required Actions of LCO 3.8.4, "DC Sources - Operating," for division(s) made inoperable by the EAS Control Instrumentation. The purpose of each referenced action is addressed in the Bases for these sections. The Completion Time of immediately is consistent with the required times for actions requiring prompt attention.

BASES

ACTIONS (continued)

K.1

Condition K applies when one or more Logic Input or Control Logic divisions are inoperable. The Required Action is to immediately enter the applicable Conditions and Required Actions of LCO 3.7.5, “Emergency Feedwater (EFW) System," for division(s) made inoperable by the EAS Control Instrumentation. The purpose of each referenced action is addressed in the Bases for these sections. The Completion Time of immediately is consistent with the required times for actions requiring prompt attention.

L.1

Condition L applies when one or more Logic Input or Control Logic divisions are inoperable. The Required Action is to immediately enter the applicable Conditions and Required Actions of LCO 3.7.9, “Safety Chilled Water (SCW) System," for division(s) made inoperable by the EAS Control Instrumentation. The purpose of each referenced action is addressed in the Bases for these sections. The Completion Time of immediately is consistent with the required times for actions requiring prompt attention.

SURVEILLANCE REQUIREMENTS

The SRs for each Function are identified by the Surveillance Requirements (SR) column of Table 3.3.10-1 for that Function. Most Functions are subject to CHANNEL CHECK, ACTUATION DEVICE OPERATIONAL TEST, CALIBRATION, SENSOR OPERATIONAL TEST, and EXTENDED SELF TESTS.

The SRs are modified by a Note. The Note directs the reader to Table 3.3.10-1 to determine the correct SRs to perform for each Function.

SR 3.3.10.1

Performance of the CHANNEL CHECK ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the 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

BASES

SURVEILLANCE REQUIREMENTS (continued)

CHECK will detect gross channel failure; therefore, it is key in verifying that the instrumentation continues to operate properly between each CALIBRATION.

Agreement criteria are determined by the plant staff, based on a combination of the channel instrument uncertainties, including isolation, indication, and readability. If a channel is outside the criteria, it may be an indication that the sensor or the signal processing equipment has drifted outside its limit. If the channels are within the criteria, it is an indication that the channels are OPERABLE.

The Frequency of 31 days is based on operating experience that demonstrates that channel failure is rare. The CHANNEL CHECK supplements less formal checks of channels during operational use of the displays associated with the LCO required channels.

SR 3.3.10.2

A SENSOR OPERATIONAL TEST (SOT) is performed every 24 months to ensure the devices will perform their intended function when needed. A SOT shall be the injection of a simulated or actual signal into the division as close to the sensor as practicable to verify OPERABILITY of all devices in the division required for division OPERABILITY. The SOT shall include the verification of the accuracy and time constants of the analog input modules.

The SOT may be performed by means of any series of sequential, overlapping, or total steps.

SR 3.3.10.3

A CALIBRATION of each sensor every 24 months ensures that each instrument division is reading accurately and within tolerance. A CALIBRATION shall be the adjustment, as necessary, of the sensor output such that it responds within the necessary range and accuracy to known values of the parameter that the division monitors. The CALIBRATION shall encompass all devices in the division required for sensor OPERABILITY.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The CALIBRATION includes provisions for the following:

1. Evaluation of sensor performance to verify that the sensor is functioning as required prior to returning the sensor to service if the as-found sensor calibration setting values are outside their predefined as-found tolerance for the specified calibration settings (e.g., 0, 25, 50, 75, and 100 percent), but conservative with respect to the Allowable Value, and

2. Declaring the sensor immediately inoperable if the sensor cannot be calibrated such that the as-left sensor calibration setting values are within the specified as-left tolerance around the specified calibration settings (e.g., 0, 25, 50, 75, and 100 percent), at the completion of the surveillance.

The CALIBRATION may be performed by means of any series of sequential, overlapping, or total steps.

SR 3.3.10.4

The features of continuous self-monitoring of the SAS are described in Reference 3. Additional tests, which require the function processor to be inoperable are not normally performed during operation. These EXTENDED SELF TESTS are performed at start-up of a function processor each cycle. The startup sequence is as follows:

– Hardware basic test using the internal diagnosis monitor,
– Start-up self-test of the operating system, and
– Switch over to normal operation after approximately two minutes.

Additional information is provided in Section 2 of Reference 3.

SR 3.3.10.5

SR 3.3.10.5 is the performance of an ADOT every 24 months. This test shall verify OPERABILITY by actuation of the RTBs and RTCs. The ADOT may be performed by means of any series of sequential, overlapping, or total steps.

BASES

REFERENCES

1. ANP-10309P, Revision 4, “U.S. EPR Protection System Technical Report,” AREVA NP Inc., May 2012.

2. FSAR, Section 7.1.

3. ANP-10315, Revision 2, “U.S. EPR Surveillance Testing and TELEPERM XS Self-Monitoring Technical Report.”]

B 3.3 INSTRUMENTATION

B 3.3.11 Post Accident Monitoring (PAM) Instrumentation

BASES

BACKGROUND

The primary purpose of the PAM instrumentation is to provide operators with information that is needed during accidents.

The OPERABILITY of PAM instrumentation ensures that there is sufficient information available on selected plant parameters to monitor and assess plant status and behavior following accidents and transients when the use of the Emergency Operating Procedures (EOP) is required as discussed in NUREG-0737, Supplement 1 (TMI Action Plan) (Reference 1).

The PAM instrumentation is required for the following reasons:

– Perform the diagnosis specified in the emergency operating procedures (these variables are restricted to preplanned actions for the primary success path of DBAs), e.g., loss of coolant accident (LOCA);
– Take the specified, pre-planned, manually controlled actions, for which no automatic control is provided, and that are required for safety systems to accomplish their safety function;
– Provide information to indicate whether plant safety functions are being accomplished for reactivity control, core cooling, maintaining reactor coolant system integrity, and maintaining containment integrity (including radioactive effluent control);
– Provide information to indicate the potential for being breached or the actual breach of the barriers to fission product releases (i.e., fuel cladding, primary coolant pressure boundary, and containment); and
– Enable the operator to recognize which heat transfer symptom is occurring: 1) loss of subcooling margin, 2) lack of heat transfer, 3) excessive heat transfer, and 4) Steam Generator Tube Rupture.

The PAM instrumentation is displayed through the Safety Information and Control Systems (SICS). The PAM instrumentation is implemented with dedicated, hardwired I&C. The PS and SAS provide the inputs to the SICS.

BASES

BACKGROUND (continued)

As long as adequate subcooling margin exists, core cooling is ensured. If subcooling margin is lost, actions are required to ensure core cooling and restore adequate subcooling margin.

The following PAM instrumentation is included in LCO 3.3.11, however, more restrictive or additional operability requirements for the associated components may be contained in LCO 3.3.1, "Reactor Trip Instrumentation," LCO 3.3.2, “Engineered Safety Feature Actuation System (ESFAS) Instrumentation,” or LCO 3.3.4, “Containment Isolation Instrumentation”:

– Cold Leg Temperature (Wide Range),
– Containment Service Compartment Pressure (Wide Range),
– Hot Leg Pressure (Wide Range),
– Hot Leg Temperature (Wide Range),
– Intermediate Range Detectors,
– Pressurizer Level (Narrow Range).
– Radiation Monitor - Containment High Range,
– Steam Generator (SG) Level (Wide Range), and
– SG Pressure.

The specific PAM instrumentation Functions listed in Table 3.3.11-1 are discussed in the LCO section.

APPLICABLE SAFETY ANALYSES

The PAM instrumentation ensures the OPERABILITY of Regulatory Guide 1.97 (Reference 2) / IEEE Standard 497-2002 (Reference 3) Type A, B, and C variables, so that the control room operating staff can:

– Recognize when a heat transfer symptom is occurring that would require performance of the appropriate section in the emergency operating procedures.
– Perform the diagnosis specified in the emergency operating procedures (these variables are restricted to preplanned actions for the primary success path of postulated accidents), e.g., loss of coolant accident (LOCA);
– Take the specified, pre-planned, manually controlled actions, for which no automatic control is provided, and that are required for safety systems to accomplish their safety function;

BASES

APPLICABLE SAFETY ANALYSIS (continued)

– Determine whether systems important to safety are performing their intended functions for reactivity control, core cooling, maintaining reactor coolant system integrity and maintaining containment integrity,
– Determine the likelihood of a gross breach of the barriers to radioactivity release;
– Determine if a gross breach of a barrier has occurred; and
– Initiate action necessary to protect the public and to estimate the magnitude of any impending threat.

PAM instrumentation used to support pre-planned, manually controlled actions satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii). The other PAM instrumentation that perform certain functions related to verification of key safety functions and monitoring key barriers for potential breach must be retained in the Technical Specifications because it is intended to assist operators in minimizing the consequences of accidents. Therefore, these variables are important for reducing public risk and satisfy Criterion 4 of 10 CFR 50.36(c)(2)(ii).

LCO

The PAM instrumentation LCO provides OPERABILITY requirements for Regulatory Guide 1.97 indicators that provide information required by the control room operators to perform certain manual actions specified in the plant Emergency Operating Procedures. These manual actions ensure that a system can accomplish its safety function, and are credited in the safety analyses. Additionally, this LCO addresses Regulatory Guide 1.97 instruments that perform certain functions related to verification of key safety functions and monitoring key barriers for potential breach.

The OPERABILITY of the PAM instrumentation ensures there is sufficient information available on selected plant parameters to monitor and assess plant status following an accident.

LCO 3.3.11 requires two OPERABLE channels for most Functions. Two OPERABLE channels ensure no single failure prevents operators from getting the information necessary for them to determine the safety status of the plant, and to bring the plant to and maintain it in a safe condition following an accident.

BASES

LCO (continued)

Furthermore, OPERABILITY of two channels allows for a comparison during the post-accident phase to confirm the validity of displayed information.

The noted exception to the two channel requirement is Containment Isolation Valve (CIV) Position Indication. In this case, the important information is the status of the containment penetrations. The LCO requires one position indication channel for each active CIV. 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 a passive valve, or via system boundary status. If a normally active CIV 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. Similarly, only one position indication channel is required for penetration flow paths with only one installed control room indication channel. This is sufficient to verify the isolation status of each penetration.

Table 3.3.11-1 provides a list of Functions identified by the Regulatory Guide 1.97 (Ref. 1) analyses. A description of the methodology used for the selection of the PAM variables is provided in FSAR Section 7.5.2.2.1 (Reference 4). Type A, B, and C variables are required to meet Regulatory Guide 1.97 design and qualification requirements for seismic and environmental qualification, single failure criterion, utilization of emergency standby power, immediately accessible display, continuous readout, and recording of display.

Listed below are discussions of the specified Functions listed in Table 3.3.11-1:

1. Cold Leg Temperature (Wide Range)

RCS cold leg temperature is used to support a credited operator manual action to control the extended partial cooldown during a Steam Generator Tube Rupture (SGTR) event when forced flow exists. It is also used to initiate actions to prevent violating reactor coolant system pressure-temperature limits and low temperature overpressure protection limits.

Four channels of Cold Leg Temperature (Wide Range) indication are provided with a range of 32°F to 662°F.

BASES

LCO (continued)

2. Containment Isolation Valve Position Indication

The containment isolation valve (CIV) position indication is used to assess containment integrity.

In the case of CIV position, the important information is the isolation status of the containment penetration. One channel of valve position indication is required to be available in the control room for each active CIV in a containment penetration flow path, (i.e., two total channels of CIV position indication for a penetration flow path with two active valves). For penetrations with only one active CIV having control room indication, Note (b) of Table 3.3.2-1 requires a single channel of valve position indication. This is to redundantly verify the isolation status of each isolable penetration via indicated status of the active valve, as applicable, and prior knowledge of passive or system boundary status. If a penetration flow path is isolated, position indication for the CIV(s) in the associated penetration flow path is not needed to determine status. Therefore, the position indication for valves in an isolated penetration flow path is not required. 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.

3. Containment Service Compartment Pressure (Wide Range)

Containment service compartment pressure is used to assess the potential challenge to containment integrity and for verification of adequate containment cooling function.

Four channels of Containment Service Compartment Pressure (Wide Range) indication are provided with a range of -5 to 220 psig.

4. Core Outlet Thermocouples (Wide Range)

Core Outlet Thermocouples are provided for monitoring Reactor Coolant System (RCS) temperature at the outlet of the core. These thermocouples are used to evaluate the status of reactor core cooling and to indicate the potential for breach of the fuel cladding.

BASES

LCO (continued)

The Core Outlet Thermocouples are distributed as homogeneously as possible across the core to provide representative indication of core outlet temperatures. The core is divided into two radial regions. The inner radial region is divided into four azimuthal zones, and the outer radial region is divided into eight azimuthal zones. One Core Outlet Thermocouple is provided in each of these 12 zones.

Each of the four channels acquires one Core Outlet Thermocouple measurement at three locations distributed radially and azimuthally in the core. Each channel acquires Core Outlet Thermocouples measurements from one zone in the inner radial region of the core, and two zones in the outer radial region of the core. The Core Outlet Thermocouples measurement location assignments are made such that each channel monitors Core Outlet Thermocouples temperatures over a wide area of the core. The Core Outlet Thermocouples assignment ensures that each channel is capable of providing indication of radial and azimuthal differences in core outlet temperatures that could be caused by factors such as radial decay power distribution, condensate runback in the hot legs, and non-uniform inlet temperatures.

Three Core Outlet Thermocouple indication is provided for each core quadrant with a range of 32°F to 2300°F.

5. Emergency Feedwater Flow to Steam Generator

Emergency Feedwater (EFW) flow is used by the operator to identify which SGs are supplied by EFW in order to determine which reactor coolant pumps should be stopped during a feedwater line break event. They are also used to determine the status of core heat removal.

Each EFW train has two channels of EFW Flow indication with a range of 0 to 545 gpm.

6. Hot Leg Pressure (Wide Range)

RCS hot leg pressure is used to control RCS pressure during the extended partial cooldown and subsequent cooldown, and in management of the Medium Head Safety Injection (MHSI) System, during an SGTR event. This instrumentation is also used to control RCS pressure during post accident cooldown to residual heat removal (RHR) conditions, and to detect RHR entry conditions.

BASES

LCO (continued)

RCS hot leg pressure is also used in conjunction with RCS cold leg temperature (T_{cold}) to detect conditions approaching RCS Nil-Ductility Transition or Pressurized Thermal Shock limits, and in conjunction with Core Outlet Thermocouples to detect inadequate core cooling.

RCS hot leg pressure is also used to provide extended range primary information to the control room operators to indicate potential or actual breach of the RCS pressure boundary.

Four channels of Hot Leg Pressure (Wide Range) indication are provided with a range of 0 to 3000 psig.

7. Hot Leg Temperature (Wide Range)

RCS hot leg temperature is used to detect RHR entry conditions to support manual operator actions to initiate RHR operation during post accident cooldown.

Four channels of Hot Leg Temperature (Wide Range) indication are provided with a range of 32°F to 662°F.

8. Intermediate Range Detector Flux

Intermediate Range Detectors are used to detect Anticipated Transient Without Scram events to support contingency actions to manually actuate the Extra Boration System within 30 minutes. This instrumentation is also used post-trip to verify the reactor is shut down.

Four channels of Intermediate Range Detectors are provided with a range of 5E-6 to 60% RTP.

9. Low Head Safety Injection Flow (Wide Range)

Low Head Safety Injection (LHSI) flow is the primary indicator of LHSI performance; it is used for initiation of contingency actions for insufficient LHSI flow. Safety Injection performance is the only valid indication of sufficient core cooling during loss of subcooling margin.

Two channels of LHSI Flow (Wide Range) indication are provided for each of the four LHSI trains with a range of 0 to 3800 gpm.

BASES

LCO (continued)

10. Medium Head Safety Injection Flow (Wide Range)

Medium Head Safety Injection (MHSI) flow is the primary indicator of MHSI performance; it is used for initiation of contingency actions for insufficient MHSI flow. Safety Injection performance is the only valid indication of sufficient core cooling during loss of subcooling margin.

Two channels of MHSI Flow (Wide Range) indication are provided for each of the four MHSI trains with a range of 0 to 1300 gpm.

11. Pressurizer Level (Narrow Range)

Pressurizer level is used to support credited operator manual actions to manage MHSI during an SGTR, and to detect an RCS inventory control upset during the Extra Boration System malfunction event. Pressurizer level is also used to provide information to the operator on the magnitude of an RCS pressure boundary breach in order to support Safety Injection management actions.

Four channels of Pressurizer Level (Narrow Range) indication are provided with a range of 0 to 100%.

12. Radiation Monitor - Annulus Ventilation System Gamma Activity

These monitors are used to determine the activity present in the exhaust air from the Annulus Ventilation System downstream of the filters to detect a breach of the containment building. This monitor is used for fission product barrier breach detection.

Two channels of Radiation Monitor - Annulus Ventilation System Gamma Activity indication are provided with a range of 1E-4 to 1E+4 rad/hr.

13. Radiation Monitor - Containment High Range

These monitors support the Radioactive Effluent Control Critical Safety Function by providing indication of the potential release source. These monitors also indicate the potential for breach or the actual breach of the fuel cladding and primary coolant boundary.

Four channels of Radiation Monitor - Containment High Range indication are provided with a range of 1E-1 to 1E+7 rad/hr.

BASES

LCO (continued)

14. Radiation Monitor - Main Steam Line

These monitors are used to detect an SGTR at power and to identify the affected SG in order to support credited operator manual actions for SGTR mitigation.

Four channels of Radiation Monitor - Main Steam Line indication are provided for each steam line with a range of 1E-8 to 1E-2 µCi/cc.

15. Steam Generator Level (Wide Range)

SG level is used to detect SG overfill and to initiate actions to prevent liquid relief through the Main Steam Safety Valves and Main Steam Relief Trains during an SGTR event. This indication is also one of the instruments utilized to detect a loss of secondary heat sink, which requires the operator to initiate feed and bleed cooling.

SG level is also provided to aid in the monitoring of primary to secondary heat transfer, to determine the need for EFW actuation, and to monitor the performance of SG level control. This instrumentation is also used to initiate actions to mitigate upsets in these functions.

Four channels of SG Level (Wide Range) indication are provided per SG with a range of 0 to 100%.

16. Steam Generator Pressure

SG pressure is used to support manual operator actions during a Feedwater Line Break (FWLB). This instrumentation is also used to determine required SG pressure and to control SG pressure when establishing SGs as a heat sink. SG pressure instrumentation is also provided to aid in the monitoring and control of primary to secondary heat transfer, in the verification that the SG is available as a heat sink, and to determine when SG isolation is required.

Four channels of SG Pressure indication are provided per SG and with range of 0 to 1600 psig.

BASES

LCO (continued)

17. Source Range Detector Flux

Source Range Detectors provide for long term surveillance of core reactivity to assess: 1) whether a return to criticality is approached during plant cooldown, 2) the need for mitigation efforts to maintain the reactor in a shutdown condition.

Three channels of Source Range Detectors are provided with a range of 0.05 to 5E+4 n/cm^2-s.

18. Subcooling Margin

The subcooling margin instrumentation (SMI) provides the operators with a numerical value of the margin to saturation at the core outlet in terms of degrees Fahrenheit. The SMI calculates how many degrees below the saturation temperature (if any) the core outlet temperature is through using the temperature at the core outlet and the hot leg pressure. The SMI is used to determine whether subcooled, saturated, or superheated conditions exist in the RCS. This information is used in the management of safety injection during an event. Both narrow and wide ranges are used in order to provide the most accurate core outlet temperature and hot leg pressure. Containment pressure is also considered in the SMI. Since the hot leg pressure sensors measure differential pressure between the hot leg and the containment atmosphere, the containment's absolute pressure is used to correct the hot leg pressure.

SMI supports manual actions to align hot leg injection after a Loss of Coolant Accident and to manage MHSI after an SGTR. Subcooling margin is also used to determine when conditions requiring full MHSI are present, and to determine if the conditions that require hot leg injection exist.

Four channels of SMI are provided with a range of 611°F Subcooling Margin to 2088°F Superheat.

[19. Site-specific Variables]

----------REVIEWER'S NOTE----------
Site-specific PAM variables will be provided by the COL applicant for site-specific Type A, B, and C parameters that meet the selection criteria in IEEE 497-2002.

BASES

APPLICABILITY

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

ACTIONS

A Note has been added in the ACTIONS to clarify the application of Completion Time rules. The Conditions of this Specification may be entered independently for each Function. The Completion Time(s) of the inoperable channel(s) of a Function will be tracked separately for each Function starting from the time the Condition was entered for that Function.

A.1

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

B.1

This Required Action specifies initiation of actions in accordance with Specification 5.6.5, which requires a written report to be submitted to the Nuclear Regulatory Commission. This report discusses the results of the root cause evaluation of the inoperability and identifies proposed restorative Required Actions. This Required Action is appropriate in lieu of a shutdown requirement, given the likelihood of plant conditions that would require information provided by this instrumentation. Also, alternative Required Actions are identified before a loss of OPERABILITY condition occurs.

BASES

ACTIONS (continued)

C.1

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

D.1

Condition D applies when the Required Action and associated Completion Time of Condition C is not met. Required Action D.1 requires entering the appropriate Condition referenced in Table 3.3.11-1 for the channel immediately. The applicable Condition referenced in the Table is Function dependent. Each time an inoperable channel has not met 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. The Completion Time of immediately is consistent with the required times for actions requiring prompt attention.

E.1 and E.2

If the Required Action and associated Completion Time of Condition C is not met and Table 3.3.11-1 directs entry into Condition E, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 4 within 12 hours.

The 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

ACTIONS (continued)

----------REVIEWER'S NOTE----------
The following Bases applies to plants that have developed, tested and obtained NRC approval to utilize a pre-planned alternate method of monitoring the normal PAM function when one or more required PAM functions have less than the minimum required channels OPERABLE.

[F.1

Alternate means of monitoring (Specify Functions) have been developed and may be temporarily installed if the normal PAM channel cannot be restored to OPERABLE status within the allowed time. If these alternate means are used, the Required Action is not to shut down the plant but rather to follow the directions of Specification 5.6.5. The report provided to the NRC should discuss the alternate means used, describe the degree to which the alternate means are equivalent to the installed PAM channels, justify the areas in which they are not equivalent, and provide a schedule for restoring the normal PAM channels.]

SURVEILLANCE REQUIREMENTS

The SRs are modified by a Note. The CHANNEL CHECK and CALIBRATION Surveillance Requirements (SR) apply to each PAM Instrumentation Function.

SR 3.3.11.1

Performance of the CHANNEL CHECK ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the 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; therefore, it is key in verifying that the instrumentation continues to operate properly between each CALIBRATION.

BASES

SURVEILLANCE REQUIREMENTS (continued)

Agreement criteria are determined by the plant staff, based on a combination of the channel instrument uncertainties, including isolation, indication, and readability. If a channel is outside the criteria, it may be an indication that the sensor or the signal processing equipment has drifted outside its limit. If the channels are within the criteria, it is an indication that the channels are OPERABLE.

As specified in the SR, a CHANNEL CHECK is only required for those channels that are normally energized.

The Frequency of 31 days is based on operating experience that demonstrates that channel failure is rare. The CHANNEL CHECK supplements less formal checks of channels during operational use of the displays associated with the LCO required channels.

SR 3.3.11.2

A CALIBRATION shall be the adjustment, as necessary, of the channel output such that it responds within the necessary range and accuracy to known values of the parameter that the channel monitors. The CALIBRATION shall encompass all devices in the channel required for channel OPERABILITY. CALIBRATION of instrument channels with resistance temperature detector (RTD) or thermocouple sensors may consist of an in-place qualitative assessment of sensor behavior and normal CALIBRATION of the remaining adjustable devices in the channel. The CALIBRATION may be performed by means of any series of sequential, overlapping, or total steps.

This SR is modified by a Note stating that neutron detectors are excluded from the CALIBRATION. The CALIBRATION for the Source Range Detectors consists of obtaining the detector plateau or preamp discriminator curves, evaluating those curves, and comparing the curves to the manufacturer's data. This Surveillance is not required for the Intermediate Range Detectors for entry into MODE 2, because the plant must be in at least MODE 2 to perform the test for the Intermediate Range Detectors.

The Frequency is based upon operating experience and consistency with the typical industry refueling cycle. The Frequency is justified by the assumption of a 24 month CALIBRATION interval for the determination of the magnitude of equipment drift.

BASES

REFERENCES

1. NUREG 0737, Supplement 1 (TMI Action Plan).
2. Regulatory Guide 1.97, Revision 4, June 2006.
3. IEEE 497-2002.
4. FSAR Section 7.5.

B 3.3 INSTRUMENTATION

B 3.3.12 Remote Shutdown Station (RSS)

BASES

BACKGROUND

The RSS 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 main control room (MCR). This capability is necessary to protect against the possibility that the MCR becomes inaccessible. A safe shutdown condition is defined as Hot Standby (MODE 3). With the plant in MODE 3, the Emergency Feedwater System (EFW) and Main Steam Relief Train can be used to remove core decay heat and meet all safety requirements. The long term supply of water for the EFW System and the ability to borate the Reactor Coolant System (RCS) from outside the MCR allow extended operation in MODE 3.

The RSS contains the Human Machine Interface (HMI) necessary to bring the plant to and maintain it in a safe shutdown state. The HMI (control) functions of the RSS are isolated as long as the MCR is available. The HMI in the RSS will continue to display all parameters available in the MCR while the control functions are isolated. The RSS HMI consists of Process Information and Control System (PICS) equipment, Safety Information and Control System (SICS) equipment (manual actuation switches), and select communication equipment. The PICS consists primarily of processing units, external units, operator workstations (OWS), plant overview panels, the automation bus, and a firewall. The PICS is used to control both safety-related and non-safely-related process systems. The plant annunciator is integrated into the PICS operating and monitoring system. Special screens display and organize alarms and warnings based on their status and relative level of importance. The SICS provides limited control capabilities in the RSS. The controls and indications on the RSS SICS are implemented with dedicated, hardwired I&C. The RSS SICS only has those manual permissives needed to reach and maintain safe shutdown.

In the event that the MCR becomes inaccessible, the operators can establish control at the RSS and place and maintain the plant in MODE 3 using the RSS PICS and RSS SICS. The plant 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 RSS ensures that there is sufficient information available on selected plant parameters to bring the plant to, and maintain it in, MODE 3 should the MCR become inaccessible.

BASES

APPLICABLE SAFETY ANALYSES

The RSS is located outside the MCR with a capability to promptly shut down the plant and maintain it in a safe condition in MODE 3.

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

The RSS satisfies Criterion 4 of 10 CFR 50.36(c)(2)(ii).

LCO

The RSS LCO provides the requirements for the OPERABILITY of the instrumentation and controls necessary to place and maintain the plant in MODE 3 from a location other than the MCR.

The controls, instrumentation, and transfer switches necessary to reach MODE 3 are those required for:

– Reactivity Control (initial and long term),
– Reactor Coolant Make-up,
– RCS Pressure Control,
– Decay Heat Removal, and
– Safety support systems for the above Functions, as well as essential service water, component cooling water, and onsite power including the Emergency Diesel Generators.

The displays and controls at the RSS are functionally the same as the displays and controls normally used by the operator to achieve and maintain MODE 3 from the MCR.

1. Transfer of Control

In the event of a condition requiring MCR evacuation, operators will transfer control from the MCR to the RSS via the MCR-RSS Transfer Switches. The MCR-RSS Transfer Switches disable MCR controls and enable control functions from the RSS. In the event that the MCR is not available and evacuation is necessary, the PICS and selected SICS controls are designed to achieve and maintain safe shutdown conditions from the RSS. The Operator Terminals for the OWS installed in the MCR will be disabled and the operators will transfer control to the OWS in the RSS. This will prevent simultaneous or unauthorized control from the MCR OWS.

The remote shutdown instrument and control circuits covered by this LCO do not need to be energized to be considered OPERABLE. This LCO is intended to ensure the instruments and control circuits will be OPERABLE if plant conditions require that the RSS be placed in operation.

BASES

APPLICABILITY

The RSS LCO is applicable in MODES 1, 2, and 3. 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 MCR.

This LCO is not applicable in MODE 4, 5, or 6. In these MODES, the plant is already subcritical and in the condition of reduced RCS energy. Under these conditions, considerable time is available to restore necessary instrument control Functions if MCR instruments or controls become unavailable.

ACTIONS

A Note has been added in the ACTIONS to clarify the application of Completion Time rules. The Conditions of this Specification may be entered independently for each MCR-RSS Transfer Switch or Function. The Completion Time(s) of the inoperable Transfer Switch(es) or Function(s) will be tracked separately for each Transfer Switch or Function starting from the time the Condition was entered for that Transfer Switch or Function.

A.1

Condition A addresses the situation where one or more MCR-RSS Transfer Switches are inoperable.

The Required Action is to restore the MCR-RSS Transfer Switch to OPERABLE status. The Completion Time of 30 days is based on operating experience and the low probability of an event that would require evacuation of the MCR.

B.1

Condition B addresses the situation where one or more Functions referenced in Table 3.3.12-1 are inoperable.

The Required Action is to restore the Function(s) to OPERABLE status. The Completion Time of 30 days is based on operating experience and the low probability of an event that would require evacuation of the MCR.

BASES

ACTIONS (continued)

C.1

Condition C addresses the situation where the RSS PICS hardware and software are inoperable.

The Required Action is to restore the RSS PICS hardware and software to OPERABLE status. The Completion Time of 30 days is based on operating experience and the low probability of an event that would require evacuation of the MCR.

D.1 and D.2

If the Required Action and associated Completion Time of Condition A, B, or C are not met, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 4 within 12 hours. The Completion Times are reasonable, based on operating experience, to reach the required MODE from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.3.12.1

SR 3.3.12.1 is the performance of an ADOT on the MCR-RSS Transfer Switches. SR 3.3.12.1 verifies that each required MCR-RSS transfer switch and control circuit performs its intended function. This verification is performed from the RSS. Operation of the equipment from the RSS is not necessary. Displays in the MCR and RSS contain real time plant data prior to, during, and after control transfer from the MCR to the RSS. The RSS data is populated from the same information busses that supply data to the MCR. During the time control is transferred from the MCR to the RSS or vice versa, the operator will have seamless transfer of control and data will not be interrupted. The operators will have an indication via the control system that RSS control has been established. This will ensure that if the MCR becomes inaccessible, the plant can be brought to and maintained in MODE 3 from the RSS. 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 demonstrates that RSS control usually passes the Surveillance when performed at a Frequency of once every 24 months

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.12.2

SR 3.3.12.2 is the performance of an ADOT every 24 months on the RSS SICS manual actuation switches. The ADOT may be performed by means of any series of sequential, overlapping, or total steps.

SR 3.3.12.3

This Surveillance verifies that the RSS communicates with the controls and indications for each division of the PICS (i.e., the operator can select the controls and indications available through each PICS division).

This Surveillance verifies the OPERABILITY of the RSS PICS hardware and software by performing diagnostics to show that operator displays are capable of being called up and displayed to an operator at the RSS. The RSS has video display units which can be used by the operator. The operator can display information on the video display units in the same manner in which the information is displayed in the MCR . The operator normally selects an appropriate set of displays based on the particular operational goals being controlled by the operator at the time. The Frequency of 24 months is based on: (1) the use of the data display capability in the MCR as part of the normal plant operation and the availability of multiple video display units at the RSS, and (2) operating experience and consistency with MCR hardware and software.

REFERENCES 1. CFR 50, Appendix A, GDC 19.

B 3.3 INSTRUMENTATION

B 3.3.13 Diverse Actuation Instrumentation

BASES

BACKGROUND

The Diverse Actuation Instrumentation provides non-Class 1E backup controls in case of beyond design basis Anticipated Transient Without Scram events or a software common cause failure (SWCCF) of the Protection System (PS). The Diverse Actuation Instrumentation is not credited for mitigating accidents in the FSAR Chapter 15 analyses.

The Diverse Actuation Instrumentation executes diverse actuation of reactor trip, engineered safety feature (ESF), and permissive functions listed in Table 3.3.13-1, and provides alarm and display functions. Sensor information is acquired by the Diverse Actuation Instrumentation from the Signal Conditioning and Distribution System (SCDS) using a hardwired signal that is not affected by a SWCCF. The Diverse Actuation Instrumentation also processes the manual, system-level actuation of critical safety functions for reactor trip, EFWS actuation, Safety Injection System actuation, containment isolation, and opening of the containment hydrogen mixing dampers. The Diverse Actuation Instrumentation also starts both station blackout diesels for manual loading by the operator.

For reactor trip functions, outputs from the Diverse Actuation Instrumentation are sent to the shunt trip coils of the reactor trip breakers, which are a diverse means of opening the breakers from the undervoltage coils that are actuated by the Protection System. For ESF functions, outputs are sent directly to the Priority and Actuator Control System (PACS). This path is not affected by a SWCCF of the Protection System. Outputs for turbine trip are sent directly to the Turbine Generator Instrumentation and Control (TG I&C) System via a hardwired connection (one per division). The TG I&C performs 2 out of 4 voting logic on the turbine trip signals.

The following features are implemented so that the automatic Diverse Actuation Instrumentation Functions do not interfere with Protection System Functions under normal circumstances, and so that the Protection System is given the opportunity to actuate before the Diverse Actuation Instrumentation:

– Diverse Actuation Instrumentation setpoints are selected to provide reasonable assurance that they will be reached after a corresponding Protection System setpoint is reached;
– Voting logic within the Diverse Actuation Instrumentation is such that single failures do not result in spurious actuations of the automatic Diverse Actuation Instrumentation Functions; and

BASES

BACKGROUND (continued)

– Priority logic within the PACS dictates that in the case of conflicting orders between the Protection System and the Diverse Actuation Instrumentation, the Protection System orders have a higher priority.

The Diverse Actuation Instrumentation Functions are designed in such a way that, once initiated, they proceed to completion. The Diverse Actuation Instrumentation Functions use the same techniques as the similar Protection System Functions to satisfy this requirement.

The Diverse Actuation Instrumentation is periodically tested to ensure the system will execute its functions. Sensors and function processors that are shared by the Protection System and the Diverse Actuation Instrumentation are periodically tested as part of the Protection System and are not required to be tested separately as part of the Diverse Actuation Instrumentation periodic testing.

FSAR Chapter 7 (Reference 1) provides a description of the Diverse Actuation Instrumentation.

The Diverse Actuation Instrumentation is segmented into three distinct but interconnected modules as identified below:

– Logic Input Division: The portion of the logic that reads in the plant parameter (e.g. temperatures and pressures) and provides the signal to the Diverse Logic Division. The hardware includes the sensor and conditioning equipment associated with the sensor (e.g., SCDS) up to the input of the Diverse Actuation Unit (DAU).
– Diverse Logic Division: The portion of the logic that receives the plant parameter and performs further conditioning (e.g. filters), calculations, comparison of values to setpoints, voting, and sends an actuation signal to the PACS. The hardware includes the DAU, hardwired logic downstream of the DAU, and cabling to the PACS.
– Manual Division: The portion of the logic that provides a manual input to the Diverse Logic Division (system-level) or PACS (component-level). The hardware includes the manual device (SICS pushbutton) and cabling to the Diverse Logic Division or PACS or reactor trip devices.

The PACS, performs prioritization of signals from different I&C systems, drive actuation, and monitoring plant actuators. Operability requirements for the PACS are addressed as part of the actuated component.

The electronics of the Control Rod Drive Control System (CRDCS) can switch-off the power supply of four CRDMs. The electronics of the CRDCS are non-safety-related but are the fastest switching device and allow the RTCs and the RTBs to open without stress.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

The Diverse Actuation Instrumentation is required to provide a diverse capability to trip the reactor and actuate the specified safety-related equipment. The Diverse Actuation Instrumentation is not credited for mitigating accidents in the FSAR Chapter 15 safety analyses. The Diverse Actuation Instrumentation satisfies Criterion 4 of 10 CFR 50.36(c)(2)(ii).

The Limiting Conditions for Operation (LCO) provides the requirements for the OPERABILITY of the Diverse Actuation Instrumentation Functions necessary to place the reactor in a shutdown condition, and to remove decay heat in the event that the required Protection System function processors do not function because of a SWCCF.

The Diverse Actuation Instrumentation is required to be OPERABLE in the MODES specified in Table 3.3.13-1.

The Diverse Actuation Instrumentation Functions are as follows:

1. Reactor Trips

a. High Neutron Flux (Power Range)

There are four divisions of High Neutron Flux (Power Range) Trip Function. These divisions are processed through 2 out of 4 voting logic. Four divisions of the High Neutron Flux (Power Range) Trip Function are required to be OPERABLE in MODE 1 with the D2 permissive validated.

Validation of the D2 permissive automatically enables the High Neutron Flux trip when the reactor power level is greater than approximately 10% Rated Thermal Power (RTP). When the reactor power level is below this threshold, the trip is disabled by manual inhibition of the D2 permissive.

b. Low-Low RCS Flow Rate in One Loop

There are four divisions of Low-Low RCS Flow Rate in One Loop Trip Function. These divisions are processed through 2 out of 4 voting logic. Four divisions of the Low-Low RCS Flow Rate in One Loop Trip Function are required to be OPERABLE in MODE 1 with D3 permissive validated.

Validation of the D3 permissive automatically enables the Low-Low RCS Flow Rate in One Loop trip when the reactor power level is greater than approximately 70% RTP. When the reactor power level is below this threshold, the trip is automatically disabled by inhibition of the D3 permissive.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

c. Low RCS Flow Rate in Two Loops

There are four divisions of Low RCS Flow Rate in Two Loops Trip Function. These divisions are processed through 2 out of 4 voting logic. Four divisions of the Low RCS Flow Rate in Two Loops Trip Function are required to be OPERABLE in MODE 1 with D2 permissive validated.

Validation of the D2 permissive automatically enables the Low RCS Flow Rate in Two Loops Trip Function when the reactor power level is greater than approximately 10% RTP. When the reactor power level is below this threshold, the trip is disabled by manual inhibition of the D2 permissive.

d. High Pressurizer Pressure

There are four divisions of High Pressurizer Pressure Trip Function. These divisions are processed through 2 out of 4 voting logic. Four divisions of the High Pressurizer Pressure Trip Function are required to be OPERABLE in MODE 1 with the D2 permissive validated.

Validation of the D2 permissive automatically enables the High Pressurizer Pressure trip when the reactor power level is greater than approximately 10% RTP. When the reactor power level is below this threshold, the trip is disabled by manual inhibition of the D2 permissive.

e. Low Hot Leg Pressure

There are four divisions of Low Hot Leg Pressure Trip Function. These divisions are processed through 2 out of 4 voting logic. Four divisions of the Low Hot Leg Pressure Trip Function are required to be OPERABLE in MODE 1 with the D2 permissive validated.

Validation of the D2 permissive automatically enables the Low Hot Leg Pressure Trip Function when the reactor power level is greater than approximately 10% RTP. When the reactor power level is below this threshold, the trip is disabled by manual inhibition of the D2 permissive.

f. Low Steam Generator (SG) Pressure

There are four divisions of Low SG Pressure Trip Function. These divisions are processed through 2 out of 4 voting logic. Four divisions of the Low SG Pressure Trip Function are required to be OPERABLE in MODE 1 with the D2 permissive validated.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

Validation of the D2 permissive automatically enables the Low SG Pressure Trip Function when the reactor power level is greater than approximately 10% RTP. When the reactor power level is below this threshold, the trip is disabled by manual inhibition of the D2 permissive.

g. Low SG Level

There are four divisions of Low SG Level Trip Function. These divisions are processed through 2 out of 4 voting logic. Four divisions of the Low SG Level Trip Function are required to be OPERABLE in MODE 1 with the D2 permissive validated.

Validation of the D2 permissive automatically enables the Low SG Level Trip Function when the reactor power level is greater than approximately 10% RTP. When the reactor power level is below this threshold, the trip is disabled by manual inhibition of the D2 permissive.

h. High SG Level

There are four divisions of High SG Level Trip Function. These divisions are processed through 2 out of 4 voting logic. Four divisions of the High SG Level Trip Function are required to be OPERABLE in MODE 1 with the D2 permissive validated.

Validation of the D2 permissive automatically enables the High SG Level Trip Function when the reactor power level is greater than approximately 10% RTP. When the reactor power level is below this threshold, the trip is disabled by manual inhibition of the D2 permissive.

i. Manual

There are four divisions of Manual Trip Function. Four divisions of the Manual Trip Function are required to be OPERABLE in MODE 1 with the D2 permissive validated.

j. Reactor Trip Breakers Shunt Trip Coils

There are two Reactor Trip Breakers Shunt Trip Coils per division. The Reactor Trip Breakers Shunt Trip Coils are required to be OPERABLE in MODE 1 with the D2 permissive validated.

These trip actuation devices support the reactor trip functions.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

i. Manual

There are four divisions of Manual Trip Function. Four divisions of the Manual Trip Function are required to be OPERABLE in MODE 1 with the D2 permissive validated.

j. Reactor Trip Breakers Shunt Trip Coils

There are two Reactor Trip Breakers Shunt Trip Coils per division. The Reactor Trip Breakers Shunt Trip Coils are required to be OPERABLE in MODE 1 with the D2 permissive validated.

These trip actuation devices support the reactor trip functions.

2. Turbine Trip

a. Reactor Trip Initiation

There are four divisions of Turbine Trip on Reactor Trip Initiation Function. These divisions are processed through 2 out of 4 voting logic. Four divisions of the automatic Turbine Trip on Reactor Trip Initiation function are required to be OPERABLE in MODES 1 and 2.

Validation of the D2 permissive automatically enables the Turbine Trip on Reactor Trip Initiation Function when the reactor power level is greater than approximately 10% RTP. When the reactor power level is below this threshold, the function is disabled by manual inhibition of the D2 permissive.

3. Safety Injection Actuation

a. Low Pressurizer Pressure

There are four divisions of SIS Actuation on Low Pressurizer Pressure Function. These divisions are processed through 2 out of 4 voting logic. Four divisions of the SIS Actuation on Low Pressurizer Pressure Function are required to be OPERABLE in MODE 1 with the D2 permissive validated.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

Validation of the D2 permissive automatically enables the SIS Actuation on Low Pressurizer Pressure Function when the reactor power level is greater than approximately 10% RTP. When the reactor power level is below this threshold, the function is disabled by manual inhibition of the D2 permissive.

b. Manual

There are four divisions of the Manual actuation Function. Four divisions of the Manual actuation Function are required to be OPERABLE in MODE 1 with the D2 permissive validated.

4. Feedwater Isolation

a. Full Load Isolation on High SG Level (Affected SG)

There are four divisions of Main Feedwater Full Load Isolation on High SG Level (Affected SG) Function. These divisions are processed through 2 out of 4 voting logic. Four divisions of the automatic Main Feedwater Full Load Isolation on High SG Level (Affected SG) Function are required to be OPERABLE in MODE 1 with the D2 permissive validated.

Validation of the D2 permissive automatically enables the Main Feedwater Full Load Isolation on High SG Level (Affected SG) Function when the reactor power level is greater than approximately 10% RTP. When the reactor power level is below this threshold, the function is disabled by manual inhibition of the D2 permissive.

b. SSS Isolation on Low SG Pressure (Affected SG)

There are four divisions of SSS Isolation on Low SG Pressure (Affected SG) Function. These divisions are processed through 2 out of 4 voting logic. Four divisions of the automatic SSS Isolation on Low SG Pressure (Affected SG) Function are required to be OPERABLE in MODE 1 with the D2 permissive validated.

Validation of the D2 permissive automatically enables the SSS Isolation on Low SG Pressure (Affected SG) Function when the reactor power level is greater than approximately 10% RTP. When the reactor power level is below this threshold, the function is disabled by manual inhibition of the D2 permissive.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

5. EFWS Actuation

a. Low SG Level (Affected SG)

There are four divisions of EFWS Actuation on Low SG Level (Affected SG) Function. These divisions are processed through 2 out of 4 voting logic. Four divisions of the automatic EFWS Actuation on Low SG Level (Affected SG) Function are required to be OPERABLE in MODE 1 with the D2 permissive validated.

Validation of the D2 permissive automatically enables the EFWS Actuation on Low SG Level (Affected SG) Function when the reactor power level is greater than approximately 10% RTP. When the reactor power level is below this threshold, the function is disabled by manual inhibition of the D2 permissive.

b. Manual

There are four divisions of Manual actuation Function. Four divisions of the Manual actuation Function are required to be OPERABLE in MODE 1 with the D2 permissive validated.

6. Main Steam Isolation

a. Low SG Pressure (All SGs)

There are four divisions of Main Steam Isolation on Low SG Pressure (All SGs) Function. These divisions are processed through 2 out of 4 voting logic. Four divisions of the automatic Main Steam Isolation on Low SG Pressure (All SGs) Function are required to be OPERABLE in MODE 1 with the D2 permissive validated.

Validation of the D2 permissive automatically enables the Main Steam Isolation on Low SG Pressure (All SGs) function when the reactor power level is greater than approximately 10% RTP. When the reactor power level is below this threshold, the function is disabled by manual inhibition of the D2 permissive.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

7. Containment Isolation (Stage 1)

a. High Containment Radiation

There are four divisions of Containment Isolation (Stage 1) on High Containment Radiation Function. These divisions are processed through 2 out of 4 voting logic. Four divisions of the automatic Containment Isolation (Stage 1) on High Containment Radiation Function are required to be OPERABLE in MODE 1 with the D2 permissive validated.

Validation of the D2 permissive automatically enables the Containment Isolation (Stage 1) on High Containment Radiation function when the reactor power level is greater than approximately 10% RTP. When the reactor power level is below this threshold, the function is disabled by manual inhibition of the D2 permissive.

b. Manual

There are four divisions of Manual actuation Function. Four divisions of the Manual actuation Function are required to be OPERABLE in MODE 1 with the D2 permissive validated.

8. Hydrogen Mixing Dampers Opening

a. High Containment Pressure

There are four divisions of Hydrogen Mixing Dampers Opening on High Containment Pressure Function. These divisions are processed through 2 out of 4 voting logic. Four divisions of the automatic Hydrogen Mixing Dampers Opening on High Containment Pressure Function are required to be OPERABLE in MODE 1 with the D2 permissive validated.

Validation of the D2 permissive automatically enables the Hydrogen Mixing Dampers Opening on High Containment Pressure Function when the reactor power level is greater than approximately 10% RTP. When the reactor power level is below this threshold, the function is disabled by manual inhibition of the D2 permissive.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

b. High Containment Compartments Delta Pressure

There are four divisions of Hydrogen Mixing Dampers Opening on High Containment Compartments Delta Pressure Function. These divisions are processed through 2 out of 4 voting logic. Four divisions of the automatic Hydrogen Mixing Dampers Opening on High Containment Compartments Delta Pressure Function are required to be OPERABLE in MODE 1 with the D2 permissive validated.

Validation of the D2 permissive automatically enables the Hydrogen Mixing Dampers Opening on High Containment Compartments Delta Pressure Function when the reactor power level is greater than approximately 10% RTP. When the reactor power level is below this threshold, the function is disabled by manual inhibition of the D2 permissive.

c. Manual

There are four divisions of Manual actuation Function. Four divisions of the Manual actuation Function are required to be OPERABLE in MODE 1 with the D2 permissive validated.

9. Station Blackout Diesels Actuation

a. Loss of Voltage

There are four divisions of Station Blackout Diesels Actuation on Loss of Voltage Function. These divisions are processed through 2 out of 4 voting logic. Four divisions of the automatic Station Blackout Diesels Actuation on Loss of Voltage Function are required to be OPERABLE in MODE 1 with the D2 permissive validated.

Validation of the D2 permissive automatically enables the Station Blackout Diesels Actuation on Loss of Voltage Function when the reactor power level is greater than approximately 10% RTP. When the reactor power level is below this threshold, the function is disabled by manual inhibition of the D2 permissive.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

10. Permissives

a. D2, Flux (Power Range) Measurement Higher than First Threshold

There are four divisions of the D2, Flux (Power Range) Measurement Higher than First Threshold Function. Four divisions of the this Function are required to be OPERABLE in MODE 1.

The D2 permissive is intended, in normal operation, to allow the operator to reach the shutdown states without inadvertent Diverse Actuation Instrumentation Function actuation. The D2 permissive uses the same excore power measurement devices as the Protection System P2 permissive.

The D2 permissive is automatically validated when the reactor power level increases above the setpoint (approximately 10% RTP) and can be manually inhibited when the reactor power level is below the setpoint. The validation of the D2 permissive automatically enables all of the Diverse Actuation Instrumentation functions except the Reactor Trip on Low-low Reactor Coolant System (RCS) Flow (One Loop). The inhibition of the D2 permissive automatically disables all of the Diverse Actuation Instrumentation functions except the Reactor Trip on Low-low RCS Flow (One Loop).

b. D3, Flux (Power Range) Measurement Higher than Second Threshold

There are four divisions of the D3, Flux (Power Range) Measurement Higher than Second Threshold Function. Four divisions of the this Function are required to be OPERABLE in MODE 1.

The D3 permissive is intended to prevent a full reactor trip actuation following a partial reactor trip due to the loss of one Reactor Coolant Pump (RCP) event. The D3 permissive uses the same excore power measurement devices as the Protection System P3 permissive.

The D3 permissive is automatically validated when the reactor power level increases above the setpoint (approximately 70% RTP) and automatically inhibited when the reactor power level decreases below the setpoint. The validation of the D3 permissive

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

automatically enables the Reactor Trip on Low-Low RCS Flow Rate in One Loop function. The inhibition of the D3 permissive automatically disables the Reactor Trip on Low-Low RCS Flow Rate in One Loop function.

11. Diverse Logic

Four divisions of the Diverse Logic Function are required to be OPERABLE in MODE 1 with the D2 permissive validated. The Diverse Logic Function consists of the portion of the logic that receives the plant parameter and performs further conditioning (e.g. filters), calculations, comparison of values to setpoints, voting, and sends an actuation signal to the PACS. The hardware includes the DAU, hardwired logic downstream of the DAU, and cabling to the PACS

12. Manual Component Switches

a. Manual Actuation of Extra Borating System (EBS)

The capability for component-level actuation of the EBS is available to the operator on the SICS in the MCR. One switch is provided per device. These switches are required to be OPERABLE in MODE 1 with the D2 permissive validated.

b. Manual actuation of Medium Head Safety Injection

One Manual actuation of Medium Head Safety Injection switch per division is required to be OPERABLE in MODE 1 with the D2 permissive validated.

c. Manual Control Room HVAC Reconfiguration

The capability for component-level actuation of the Control Room HVAC Reconfiguration switches is available to the operator on the SICS in the MCR. One switch is provided per device. These switches are required to be OPERABLE in MODE 1 with the D2 permissive validated.

d. Manual Chemical and Volume Control System Isolation

The capability for component-level actuation of the Chemical and Volume Control System Isolation is available to the operator on the SICS in the MCR. One switch is provided per device. These switches are required to be OPERABLE in MODE 1 with the D2 permissive validated.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

e. Manual depressurize Reactor Coolant System with Pressurizer Sprays

The capability for component-level depressurization of the Reactor Coolant System with Pressurizer Sprays switches is available to the operator on the SICS in the MCR. These switches are required to be OPERABLE in MODE 1 with the D2 permissive validated.

f. Manual diesel generator loading (Emergency Diesel Generators (EDG) or Station Blackout)

The capability for component-level diesel generator loading switches is available to the operator on the SICS in the MCR. These switches are required to be OPERABLE in MODE 1 with the D2 permissive validated.

g. Manual EDG start

The capability for component-level diesel generator starting is available to the operator on the SICS in the MCR. These switches are required to be OPERABLE in MODE 1 with the D2 permissive validated.

h. Manual Feedwater Isolation (Main Feedwater and Emergency Feedwater)

The capability for component-level actuation of Feedwater Isolation (Main Feedwater and Emergency Feedwater) is available to the operator on the SICS in the MCR. One switch is provided per device. These switches are required to be OPERABLE in MODE 1 with the D2 permissive validated.

i. Manual Main Steam Isolation Valve closure

The capability for component-level Main Steam Isolation Valve closure is available to the operator on the SICS in the MCR. These switches are required to be OPERABLE in MODE 1 with the D2 permissive validated.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

j. Manual Main Steam Relief Train control

The capability for component-level Main Steam Relief Train control is available to the operator on the SICS in the MCR. These switches are required to be OPERABLE in MODE 1 with the D2 permissive validated.

k. Manual operation of Emergency Feedwater for SG Level Control

The capability for component-level operation of Emergency Feedwater for SG Level Control is available to the operator on the SICS in the MCR. These switches are required to be OPERABLE in MODE 1 with the D2 permissive validated.

l. Manual Safety Injection switchover to RCS hot leg injection

The capability for component-level Safety Injection switchover to RCS hot leg injection is available to the operator on the SICS in the MCR. These switches are required to be OPERABLE in MODE 1 with the D2 permissive validated.

m. Manually extend Partial Cooldown

The capability for component-level control to extend partial cooldown switches is available to the operator on the SICS in the MCR. These switches are required to be OPERABLE in MODE 1 with the D2 permissive validated.

ACTIONS

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

A.1

Condition A applies to all Diverse Actuation Instrumentation Functions. Condition A addresses the situation where one or more Functions with one or more required divisions are inoperable. The Required Action is to refer to Table 3.3.13-1 and to take the Required Actions for the Functions affected. The Completion Times are those from the referenced Conditions and Required Actions.

BASES

ACTIONS (continued)

B.1

Condition B applies when one Logic Input division or one Diverse Logic division is inoperable. In this condition, the minimum number of OPERABLE divisions to read the plant parameter, perform conditioning, calculations, compare the values to setpoints, and sending to the voting logic during an Anticipated Operational Occurrence (AOO) or postulated accident coupled with a software common cause failure of the Protection System is still available. The Completion Time of 30 days to restore the division to OPERABLE status is reasonable considering the availability of automatic actuation and the low probability of an AOO or postulated accident coupled with a Protection System software common cause failure occurring during this time.

C.1

Condition C applies when two Logic Input divisions or two Diverse Logic divisions are inoperable. In this condition, the minimum number of OPERABLE divisions to read the plant parameter, perform conditioning, calculations, compare the values to setpoints, and sending to the voting logic during an AOO or postulated accident coupled with a software common cause failure of the Protection System is still available. The Completion Time of 72 hours to restore one division to OPERABLE status is reasonable considering the availability of automatic actuation and the low probability of an AOO or postulated accident coupled with a Protection System software common cause failure occurring during this time.

D.1

Condition D applies when one or more Manual Component Switch divisions are inoperable. The Completion Time of 30 days to restore the division(s) to OPERABLE status is reasonable considering the low probability of an AOO or postulated accident coupled with a Protection System software common cause failure occurring during this time.

BASES

ACTIONS (continued)

E.1

Condition E addresses the failure of three or more Logic Input divisions, three or more Diverse Logic divisions, or the Required Action and associated Completion Time of Condition B or C was not met. With the automatic Diverse Actuation Instrumentation function inoperable, the plant must be brought to a MODE where the trip, Actuation, isolation, logic, or manual Function is no longer required. The Completion Time of 2 hours is reasonable, based on operating experience, to reach MODE 1 with D3 inhibited in an orderly manner and without challenging plant systems.

F.1

Condition F addresses the failure of three or more Logic Input divisions, three or more Diverse Logic divisions, or the Required Action and associated Completion Time of Condition B, C, or D was not met. With the automatic or manual Diverse Actuation Instrumentation function inoperable, the plant must be brought to a MODE where the trip, Actuation, isolation, logic, or manual Function is no longer required. The Completion Time of 6 hours is reasonable, based on operating experience, to reach MODE 1 with D2 inhibited in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

The SRs for each Function are identified by the Surveillance Requirements (SR) column of Table 3.3.13-1 for that Function. Most Functions are subject to, CALIBRATION, SENSOR OPERATIONAL TEST, ACTUATION LOGIC TEST, and RESPONSE TIME testing.

The SRs are modified by a Note. The Note directs the reader to Table 3.3.13-1 to determine the correct SRs to perform for each Function.

SR 3.3.13.1

A CALIBRATION of each sensor every 24 months ensures that each instrument division is reading accurately and within tolerance. A CALIBRATION shall be the adjustment, as necessary, of the sensor output such that it responds within the necessary range and accuracy to known values of the parameter that the division monitors. The CALIBRATION shall encompass all devices in the division required for sensor OPERABILITY.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The CALIBRATION includes provisions for the following:

1. Evaluation of sensor performance to verify that the sensor is functioning as required prior to returning the sensor to service if the as-found sensor calibration setting values are outside their predefined as-found tolerance for the specified calibration settings (e.g., 0, 25, 50, 75, and 100 percent), but conservative with respect to the Allowable Value, and

2. Declaring the sensor immediately inoperable if the sensor cannot be calibrated such that the as-left sensor calibration setting values are within the specified as-left tolerance around the specified calibration settings (e.g., 0, 25, 50, 75, and 100 percent), at the completion of the surveillance.

The CALIBRATION may be performed by means of any series of sequential, overlapping, or total steps.

SR 3.3.13.2

A SENSOR OPERATIONAL TEST (SOT) is performed every 24 months to ensure the devices will perform their intended function when needed. A SOT shall be the injection of a simulated or actual signal into the division as close to the sensor as practicable to verify OPERABILITY of all devices in the division required for division OPERABILITY. The SOT shall include the verification of the accuracy and time constants of the analog input modules.

The SOT may be performed by means of any series of sequential, overlapping, or total steps.

SR 3.3.13.3

An ACTUATION LOGIC TEST is performed on the DAU. The division being tested is placed in the bypass condition, thus preventing inadvertent actuation. All possible logic combinations are tested for each function. Verification of bistable module, logic module, and output module is included in this test.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.13.4

SR 3.3.13.4 is the performance of an ACTUATING DEVICE OPERATIONAL TEST (ADOT) every 24 months. The ADOT may be performed by means of any series of sequential, overlapping, or total steps.

SR 3.3.13.5

SR 3.3.13.5 verifies that the individual division actuation response times are less than or equal to the maximum values assumed in the diversity and defense-in-depth assessment. Response time testing acceptance criteria are included in a document controlled under 10 CFR 50.59. Individual component response times are not modeled in the assessment.

The assessment models the overall or total elapsed time, from the point at which the parameter exceeds the trip setpoint value at the sensor to the point at which the equipment reaches the required functional state (i.e., control and shutdown rods fully inserted in the reactor core, pumps at rated discharge pressure, or valves in full open or closed position).

For divisions that include dynamic transfer functions (e.g., lag, lead/lag, rate/lag, etc.), the response time test may be performed with the transfer function set to one, with the resulting measured response time compared to the appropriate FSAR response time. Alternately, the response time test can be performed with the time constants set to their nominal value, provided the required response time is analytically calculated assuming the time constants are set at their nominal values. The response time may be measured by a series of overlapping tests such that the entire response time is measured.

----------REVIEWER'S NOTE----------
The following Bases apply to plants that have obtained NRC approval to utilize allocations for selected components based on NRC-approved U.S. EPR-applicable Topical Reports.

[Response time may be verified by actual response time tests in any series of sequential, overlapping or total division measurements, or by the summation of allocated sensor, signal processing and actuation logic response times with actual response time tests on the remainder of the

BASES

SURVEILLANCE REQUIREMENTS (continued)

division. Allocations for sensor response times may be obtained from: (1) historical records based on acceptable response time tests (hydraulic, noise, or power interrupt tests), (2) in place, onsite, or offsite (e.g., vendor) test measurements, or (3) utilizing vendor engineering specifications. Response time verification for other sensor types must be demonstrated by test.

The allocations for sensor, signal conditioning, and actuation logic response times must be verified prior to placing the component in operational service and re-verified following maintenance that may adversely affect response time. In general, electrical repair work does not impact response time provided the parts used for repair are of the same type and value. One example where response time could be affected is replacing the sensing assembly of a transmitter.]

As appropriate, each division's response must be verified every 24 months on a STAGGERED TEST BASIS. Testing of the final actuation devices is included in the testing. Response times cannot be determined during plant operation because equipment operation is required to measure response times. Experience has shown that these components usually pass this surveillance when performed at the 24 month Frequency. Therefore, the Frequency was concluded to be acceptable from a reliability standpoint.

SR 3.3.13.5 is modified by a Note stating that neutron detectors are excluded from RESPONSE TIME testing. The Note is necessary because of the difficulty in generating an appropriate detector input signal. Excluding the detectors is acceptable because the principles of detector operation ensure a virtually instantaneous response.

REFERENCES 1. CFR 50, Appendix A, GDC 19.

B 3.3 INSTRUMENTATION

B 3.3.14 Self-Powered Neutron Detectors (SPND)

BASES

BACKGROUND

Refer to B 3.3.1, “Reactor Trip Instrumentation,” for background information on the Distributed Control System.

The other LCOs in the Instrumentation section address Functions. This LCO addresses components.

There are 72 SPNDs that continuously measure the neutron flux at given positions in the core to provide information about the three-dimensional flux distribution. There are 12 SPND strings with six SPNDs in each string. Each SPND detector string contains six axial SPNDs, which are placed in specific radial core positions to provide information about the three dimensional neutron flux distribution inside the core.

The Aeroball Measurement System (AMS) is used to calibrate the SPNDs at regular intervals. The SPNDs and AMS are described in detail in the Incore Trip Setpoint Transient Methodology for the U.S. EPR Topical Report (ANP-10287P) (Reference 1).

All 72 SPND measurements are used in each PS division. The SPNDs are used as inputs to calculate variables that cannot be directly measured, such as linear power density and departure from nucleate boiling ratio (DNBR). Space- and time- dependent power density distribution of the U.S. EPR is accurately assessed using the SPNDs inside the core. For neutron flux measurement, incore neutron detectors are more accurate than excore neutron detectors.

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

Refer to B 3.3.1, “Reactor Trip Instrumentation,” for applicable safety analyses, LCO, and applicability information that is generically applicable to U.S. EPR systems that perform reactor trip functions.

Seventy-two of seventy-two SPNDs are required to be OPERABLE in MODE 1 with THERMAL POWER greater than or equal to 10% RATED THERMAL POWER (P2 permissive validated).

The SPNDs support the following reactor trip functions:

– Reactor Trip 1: DNBR - Low,
– Reactor Trip 2: DNBR with High Quality – Low,

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

- Reactor Trip 3: DNBR with Imbalance or Rod Drop (1/4) – Low,
- Reactor Trip 4: DNBR with High Quality and (Imbalance or Rod Drop) (1/4) – Low, and
- Reactor Trip 5: DNBR with Rod Drop (2/4) – Low, and
- Reactor Trip 6: Linear Power Density - High.

As described in Reference 1, these reactor trip Functions will accommodate a limited number of inoperable SPNDs through the use of multiple setpoints.

The SPNDs satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

ACTIONS

A.1

Condition A addresses the situation where one, two, three, four, or five SPNDs are inoperable. In this condition, the remaining OPERABLE SPNDs are still providing information regarding flux distribution within the reactor core. However, the uncertainties regarding the flux distribution change with each failed SPND. These increased uncertainties have been analyzed and the resulting penalties (or necessary changes to the reactor trip setpoints) are documented in the COLR. Updating the setpoints for the affected reactor trip Functions restores the Protection System to an analyzed state. The Completion Time of 6 hours is reasonable considering the time necessary to change the setpoints in the Protection System.

B.1

Condition B applies when six or more SPNDs are inoperable or the inability to complete the remedial measures in the time allowed by Required Actions A.1. With six or more inoperable SPNDs, the remaining OPERABLE SPNDs are still providing information regarding flux distribution within the reactor core. However, the uncertainties regarding the flux distribution change with this number of failed SPND have not been analyzed. Therefore, the plant must be brought to a MODE where the supported reactor trip Functions are not required to be OPERABLE. The Completion Time of 4 hours to reach MODE 1 with P2 inhibited is reasonable, based on operating experience, to reach the required power level from full power conditions in an orderly manner and without challenging plant systems.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.3.14.1

A CALIBRATION of each SPND every 15 effective full power days (EFPD) ensures that each instrument division is reading accurately and within tolerance. The test is performed in accordance with the Setpoint Control Program.

Space- and time- dependent power density distribution of the U.S. EPR is accurately assessed using the SPNDs inside the core. For neutron flux measurement, incore neutron detectors are more accurate than excore neutron detectors. CALIBRATION of SPND instrumentation is performed to compensate for a decrease in SPND sensitivity during the fuel cycle and to account for peak power density factor change over the fuel cycle. The Aeroball Measurement System (AMS) assists in generating the measured relative neutron flux density in the core, which is used in conjunction with the predicted power distribution based on actual core operation to calibrate the incore SPND instrumentation. Because both the power-to-signal ratio of an SPND and the reference power distribution change with core burnup, SPND signals are matched to reference signals provided by the AMS every 15 EFPDs.

Calibration of the SPNDs is performed based on flux mapping by the AMS. The principles of SPND calibration based on the AMS flux mapping are described in detail in Appendix B of ANP-10287P, "U.S. EPR Incore Trip Setpoint and Transient Methodology" (Reference 1). The resulting SPND calibration factors are entered into the Acquisition and Processing Units function processor application software via the Service Unit.

The SR is modified by a Note. The Note clarifies that 12 hours are allowed for performing the first Surveillance after reaching 20% RTP. A reactor power level of 20% RTP is chosen based on plant stability, (i.e., automatic rod control capability and turbine generator synchronized to the grid). The Frequency of every 15 EFPDs is adequate. It is based on plant operating experience, considering instrument reliability and operating history data for SPND drift.

REFERENCES

1. ANP-10287P, Revision 0, “Incore Trip Setpoint and Transient Methodology for U.S. EPR Topical Report,” AREVA NP Inc., November 2007.