B 3.3 INSTRUMENTATION

B 3.3.5.1 Emergency Core Cooling System (ECCS) Instrumentation

BASES

BACKGROUND

The purpose of the ECCS instrumentation is to initiate appropriate responses from the systems to ensure that the fuel is adequately cooled in the event of a design basis accident or transient.

For most abnormal operational transients and Design Basis Accidents (DBAs), a wide range of dependent and independent parameters are monitored.

The ECCS instrumentation actuates core spray (CS), low pressure coolant injection (LPCI), high pressure coolant injection (HPCI), Automatic Depressurization System (ADS), and the diesel generators (DGs). The equipment involved with each of these systems is described in the Bases for LCO 3.5.1, "ECCS—Operating."

Core Spray System

The CS System may be initiated by automatic means. Automatic initiation occurs for conditions of Reactor Vessel Water Level—Low Low Low (Level 1) or Drywell Pressure—High with a Reactor Pressure—Low permissive. The reactor vessel water level and the reactor pressure variables are monitored by four redundant transmitters, which are, in turn, connected to four pressure compensation instruments. The drywell pressure variable is monitored by four redundant transmitters, which are, in turn, connected to four trip units. The outputs of the pressure compensation instruments and the trip units are connected to relays which send signals to two trip systems, with each trip system arranged in a one-out-of-two taken twice logic (each trip unit sends a signal to both trip systems.) Each trip system initiates two of the four CS pumps.

Upon receipt of an initiation signal, if normal AC power is available, CS pumps A and C start after a time delay of approximately 13 seconds and CS pumps B and D start after a time delay of approximately 23 seconds. If normal AC power is not available, the four CS pumps start simultaneously after a time delay of approximately 6 seconds after the respective DG is ready to load.

(continued)

BASES

BACKGROUND

Core Spray System (continued)

The CS test line isolation valve, which is also a primary containment isolation valve (PCIV), is closed on a CS initiation signal to allow full system flow assumed in the accident analyses and maintain primary containment isolated in the event CS is not operating.

The CS pump discharge flow is monitored by a differential pressure indicating switch. When the pump is running and discharge flow is low enough so that pump overheating may occur, the minimum flow return line valve is opened. The valve is automatically closed if flow is above the minimum flow setpoint to allow the full system flow assumed in the accident analysis.

The CS System also monitors the pressure in the reactor to ensure that, before the injection valves open, the reactor pressure has fallen to a value below the CS System's maximum design pressure. The variable is monitored by four redundant transmitters, which are, in turn, connected to four pressure compensation instruments. The outputs of the pressure compensation instruments are connected to relays whose contacts are arranged in a one-out-of-two taken twice logic.

Low Pressure Coolant Injection System

The LPCI is an operating mode of the Residual Heat Removal (RHR) System, with two LPCI subsystems. The LPCI subsystems may be initiated by automatic means. Automatic initiation occurs for conditions of Reactor Vessel Water Level—Low Low Low (Level 1); Drywell Pressure—High with a Reactor Pressure—Low (Injection Permissive). The drywell pressure variable is monitored by four redundant transmitters, which, in turn, are connected to four trip units. The reactor vessel water level and the reactor pressure variables are monitored by four redundant transmitters, which are, in turn, connected to four pressure compensation instruments. The outputs of the trip units and pressure compensation instruments are connected to relays which send signals to two trip systems, with each trip system arranged in a one-out-of-two taken twice logic (each trip unit sends a signal to both trip systems). Each trip system can initiate all four LPCI pumps.

(continued)

BASES

BACKGROUND

Low Pressure Coolant Injection System (continued)

Upon receipt of an initiation signal if normal AC power is available, the LPCI A and B pumps start after a delay of approximately 2 seconds. The LPCI C and D pumps are started after a delay of approximately 8 seconds. If normal AC power is not available, the four LPCI pumps start simultaneously with no delay as soon as the standby power source is available.

Each LPCI subsystem's discharge flow is monitored by a differential pressure indicating switch. When a pump is running and discharge flow is low enough so that pump overheating may occur, the respective minimum flow return line valve is opened. If flow is above the minimum flow setpoint, the valve is automatically closed to allow the full system flow assumed in the analyses.

The RHR test line suppression pool cooling isolation valve, suppression pool spray isolation valves, and containment spray isolation valves (which are also PCIVs) are also closed on a LPCI initiation signal to allow the full system flow assumed in the accident analyses and maintain primary containment isolated in the event LPCI is not operating.

The LPCI System monitors the pressure in the reactor to ensure that, before an injection valve opens, the reactor pressure has fallen to a value below the LPCI System's maximum design pressure. The variable is monitored by four redundant transmitters, which are, in turn, connected to four pressure compensation instruments. The outputs of the pressure compensation instruments are connected to relays whose contacts are arranged in a one-out-of-two taken twice logic. Additionally, instruments are provided to close the recirculation pump discharge valves to ensure that LPCI flow does not bypass the core when it injects into the recirculation lines. The variable is monitored by four redundant transmitters, which are, in turn, connected to four pressure compensation instruments. The outputs of the pressure compensation instruments are connected to relays whose contacts are arranged in a one-out-of-two taken twice logic.

(continued)

BASES

BACKGROUND

Low Pressure Coolant Injection System (continued)

Low reactor water level in the shroud is detected by two additional instruments. When the level is greater than the low level setpoint LPCI may no longer be required, therefore other modes of RHR (e.g., suppression pool cooling) are allowed. Manual overrides for the isolations below the low level setpoint are provided.

High Pressure Coolant Injection System

The HPCI System may be initiated by automatic means. Automatic initiation occurs for conditions of Reactor Vessel Water Level—Low Low (Level 2) or Drywell Pressure—High. The reactor vessel water level variable is monitored by four redundant transmitters, which are, in turn, connected to four pressure compensation instruments. The drywell pressure variable is monitored by four redundant transmitters, which are, in turn, connected to four trip units. The outputs of the pressure compensation instruments and the trip units are connected to relays whose contacts are arranged in a one-out-of-two taken twice logic for each Function.

The HPCI pump discharge flow is monitored by a flow switch. When the pump is running and discharge flow is low enough so that pump overheating may occur, the minimum flow return line valve is opened. The valve is automatically closed if flow is above the minimum flow setpoint to allow the full system flow assumed in the safety analysis.

The HPCI test line isolation valve (which is also a PCIV) is closed upon receipt of a HPCI initiation signal to allow the full system flow assumed in the accident analysis and maintain primary containment isolated in the event HPCI is not operating.

The HPCI System also monitors the water levels in the condensate storage tank (CST) and the suppression pool because these are the two sources of water for HPCI operation. Reactor grade water in the CST is the normal source. Upon receipt of a HPCI initiation signal, the CST

(continued)

BASES

BACKGROUND

High Pressure Coolant Injection System (continued)

suction valve is automatically signaled to open (it is normally in the open position) unless both suppression pool suction valves are open. If the water level in the CST falls below a preselected level, first the suppression pool suction valves automatically open, and then the CST suction valve automatically closes. Two level switches are used to detect low water level in the CST. Either switch can cause the suppression pool suction valves to open and the CST suction valve to close. The suppression pool suction valves also automatically open and the CST suction valve closes if high water level is detected in the suppression pool. To prevent losing suction to the pump, the suction valves are interlocked so that one suction path must be open before the other automatically closes.

The HPCI provides makeup water to the reactor until the reactor vessel water level reaches the Reactor Vessel Water Level—High (Level 8) trip, at which time the HPCI turbine trips, which causes the turbine's stop valve and the control valves to close. The logic is two-out-of-two to provide high reliability of the HPCI System. The HPCI System automatically restarts if a Reactor Vessel Water Level—Low Low (Level 2) signal is subsequently received.

Automatic Depressurization System

The ADS may be initiated by automatic means. Automatic initiation occurs when signals indicating Reactor Vessel Water Level—Low Low Low (Level 1); Drywell Pressure—High or ADS Bypass Low Water Level Actuation Timer; Reactor Vessel Water Confirmatory Level—Low (Level 4); and CS or LPCI Pump Discharge Pressure—High are all present and the ADS Initiation Timer has timed out. There are two transmitters each for Reactor Vessel Water Level—Low Low Low (Level 1) and Drywell Pressure—High, and one transmitter for Reactor Vessel Water Confirmatory Level—Low (Level 4) in each of the two ADS trip systems. Each of these transmitters connects to a trip unit, which then drives a relay whose contacts form the initiation logic.

Each ADS trip system includes a time delay between satisfying the initiation logic and the actuation of the ADS valves. The ADS Initiation Timer time delay setpoint chosen is long enough that the HPCI has sufficient operating time

(continued)

BASES

BACKGROUND

Automatic Depressurization System (continued)

to recover to a level above Level 1, yet not so long that the LPCI and CS Systems are unable to adequately cool the fuel if the HPCI fails to maintain that level. An alarm in the control room is annunciated when either of the timers is timing. Resetting the ADS initiation signals resets the ADS Initiation Timers.

The ADS also monitors the discharge pressures of the four LPCI pumps and the four CS pumps. Each ADS trip system includes two discharge pressure permissive switches from all four LPCI pumps and one discharge pressure permissive switch from all four CS pumps. The signals are used as a permissive for ADS actuation, indicating that there is a source of core coolant available once the ADS has depressurized the vessel. Two CS pumps in proper combination (C or D and A or B) or any one of the four LPCI pumps is sufficient to permit automatic depressurization.

The ADS logic in each trip system is arranged in two strings. Each string has a contact from each of the following variables: Reactor Vessel Water Level—Low Low Low (Level 1); Drywell Pressure—High; Low Water Level Actuation Timer; and Reactor Vessel Water Level—Low Low Low (Level 1) Permissive. One of the two strings in each trip system must also have a Reactor Vessel Water Confirmatory Level—Low (Level 4). After the contacts for the initiation signal from either drywell pressure or reactor vessel level (and the timer for reactor vessel level timing out) close, the following must be present to initiate an ADS trip system: all other contacts in both logic strings must close, the ADS initiation timer must time out, and a CS or LPCI pump discharge pressure signal must be present. Either the A or B trip system will cause all the ADS relief valves to open. Once the Drywell Pressure—High signal, the ADS Low Water Level Actuation Timer, or the ADS initiation signal is present, it is individually sealed in until manually reset.

Manual inhibit switches are provided in the control room for the ADS; however, their function is not required for ADS OPERABILITY (provided ADS is not inhibited when required to be OPERABLE).

(continued)

BASES

BACKGROUND (continued)

Diesel Generators

The DGs may be initiated by automatic means. Automatic initiation occurs for conditions of Reactor Vessel Water Level – Low Low Low (Level 1) or Drywell Pressure – High. The DGs are also initiated upon loss of voltage signals. (Refer to the Bases for LCO 3.3.8.1, "Loss of Power (LOP) Instrumentation," for a discussion of these signals.) The reactor vessel water level variable is monitored by four redundant transmitters, which are, in turn, connected to four pressure compensation instruments. The drywell pressure variable is monitored by four redundant transmitters, which are, in turn, connected to four trip units. The outputs of the four pressure compensation instruments and the trip units are connected to relays which send signals to two trip systems, with each trip system arranged in a one-out-of-two taken twice logic (each trip unit sends a signal to both trip systems). The A trip system initiates all four DGs and the B trip system initiates all four DGs. The DGs receive their initiation signals from the CS System initiation logic. The DGs can also be started manually from the control room and locally from the associated DG room. Upon receipt of a loss of coolant accident (LOCA) initiation signal, each DG is automatically started, is ready to load in approximately 10 seconds, and will run in standby conditions (rated voltage and speed, with the DG output breaker open). The DGs will only energize their respective Engineered Safety Feature buses if a loss of offsite power occurs. (Refer to Bases for LCO 3.3.8.1.)

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

The actions of the ECCS are explicitly assumed in the safety analyses of References 1, 2, and 3. The ECCS is initiated to preserve the integrity of the fuel cladding by limiting the post LOCA peak cladding temperature to less than the 10 CFR 50.46 limits.

ECCS instrumentation satisfies Criterion 3 of the NRC Policy Statement. Certain instrumentation Functions are retained for other reasons and are described below in the individual Functions discussion.

The OPERABILITY of the ECCS instrumentation is dependent upon the OPERABILITY of the individual instrumentation channel Functions specified in Table 3.3.5.1-1. Each Function must have a required number of OPERABLE channels,

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

with their setpoints within the specified Allowable Values, where appropriate. The actual setpoint is calibrated consistent with applicable setpoint methodology assumptions. Table 3.3.5.1-1, footnote (b), is added to show that certain ECCS instrumentation Functions are also required to be OPERABLE to perform DG initiation.

Allowable Values are specified for each ECCS Function specified in the Table. Trip setpoints are specified in the setpoint calculations. The trip setpoints are selected to ensure that the settings do not exceed the Allowable Value between CHANNEL CALIBRATIONS. Operation with a trip setting less conservative than the trip setpoint, but within its Allowable Value, is acceptable. A channel is inoperable if its actual trip setpoint is not within its required Allowable Value. Trip setpoints are those predetermined values of output at which an action should take place. The setpoints are compared to the actual process parameter (e.g., reactor vessel water level), and when the measured output value of the process parameter exceeds the setpoint, the associated device (e.g., trip unit) changes state. The analytic or design limits are derived from the limiting values of the process parameters obtained from the safety analysis or other appropriate documents. The Allowable Values are derived from the analytic or design limits, corrected for calibration, process, and instrument errors. The trip setpoints are determined from analytical or design limits, corrected for calibration, process, and instrument errors, as well as, instrument drift. In selected cases, the Allowable Values and trip setpoints are determined from engineering judgement or historically accepted practice relative to the intended functions of the channel. The trip setpoints determined in this manner provide adequate protection by assuming instrument and process uncertainties expected for the environments during the operating time of the associated channels are accounted for. For the Core Spray and LPCI Pump Start-Time Delay Relays, adequate margins for applicable setpoint methodologies are incorporated into the Allowable Values and actual setpoints.

In general, the individual Functions are required to be OPERABLE in the MODES or other specified conditions that may require ECCS (or DG) initiation to mitigate the consequences of a design basis transient or accident. To ensure reliable ECCS and DG function, a combination of Functions is required to provide primary and secondary initiation signals.

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

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

Core Spray and Low Pressure Coolant Injection Systems

1.a, 2.a. Reactor Vessel Water Level—Low Low Low (Level 1)

Low reactor pressure vessel (RPV) water level indicates that the capability to cool the fuel may be threatened. Should RPV water level decrease too far, fuel damage could result. The low pressure ECCS and associated DGs are initiated at Reactor Vessel Water Level—Low Low Low (Level 1) to ensure that core spray and flooding functions are available to prevent or minimize fuel damage. The DGs are initiated from Function 1.a signals. This Function, in conjunction with a Reactor Pressure—Low (Injection Permissive) signal, also initiates the closure of the Recirculation Discharge Valves to ensure the LPCI subsystems inject into the proper RPV location. The Reactor Vessel Water Level—Low Low Low (Level 1) is one of the Functions assumed to be OPERABLE and capable of initiating the ECCS during the transients analyzed in References 1 and 3. In addition, the Reactor Vessel Water Level—Low Low Low (Level 1) Function is directly assumed in the analysis of the recirculation line break (Ref. 4) and the control rod drop accident (CRDA) analysis. The core cooling function of the ECCS, along with the scram action of the Reactor Protection System (RPS), ensures that the fuel peak cladding temperature remains below the limits of 10 CFR 50.46.

Reactor Vessel Water Level—Low Low Low (Level 1) signals are initiated from four level transmitters that sense the difference between the pressure due to a constant column of water (reference leg) and the pressure due to the actual water level (variable leg) in the vessel.

The Reactor Vessel Water Level—Low Low Low (Level 1) Allowable Value is chosen to allow time for the low pressure core flooding systems to activate and provide adequate cooling.

Four channels of Reactor Vessel Water Level—Low Low Low (Level 1) Function are only required to be OPERABLE when the ECCS or DG(s) are required to be OPERABLE to ensure that no single instrument failure can preclude ECCS and DG

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

1.a, 2.a. Reactor Vessel Water Level—Low Low Low (Level 1) (continued)

initiation. Refer to LCO 3.5.1 and LCO 3.5.2, "ECCS—Shutdown," for Applicability Bases for the low pressure ECCS subsystems; LCO 3.8.1, "AC Sources—Operating"; and LCO 3.8.2, "AC Sources—Shutdown," for Applicability Bases for the DGs.

1.b, 2.b. Drywell Pressure—High

High pressure in the drywell could indicate a break in the reactor coolant pressure boundary (RCPB). The low pressure ECCS and associated DGs are initiated upon receipt of the Drywell Pressure—High Function with a Reactor Pressure—Low (Injection Permissive) in order to minimize the possibility of fuel damage. The DGs are initiated from Function 1.b signals. This Function also initiates the closure of the recirculation discharge valves to ensure the LPCI subsystems inject into the proper RPV location. The Drywell Pressure—High Function with a Reactor Pressure—Low (Injection Permissive), along with the Reactor Water Level—Low Low Low (Level 1) Function, is directly assumed in the analysis of the recirculation line break (Ref. 4). The core cooling function of the ECCS, along with the scram action of the RPS, ensures that the fuel peak cladding temperature remains below the limits of 10 CFR 50.46.

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

The Drywell Pressure—High Function is required to be OPERABLE when the ECCS or DG is required to be OPERABLE in conjunction with times when the primary containment is required to be OPERABLE. Thus, four channels of the CS and LPCI Drywell Pressure—High Function are required to be OPERABLE in MODES 1, 2, and 3 to ensure that no single instrument failure can preclude ECCS and DG initiation. In MODES 4 and 5, the Drywell Pressure—High Function is not required, since there is insufficient energy in the reactor to pressurize the primary containment to Drywell Pressure—High setpoint. Refer to LCO 3.5.1 for Applicability Bases for the low pressure ECCS subsystems and to LCO 3.8.1 for Applicability Bases for the DGs.

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

1.c, 2.c. Reactor Pressure—Low (Injection Permissive)

Low reactor pressure signals are used as permissives for the low pressure ECCS subsystems. This ensures that, prior to opening the injection valves of the low pressure ECCS subsystems or initiating the low pressure ECCS subsystems on a Drywell Pressure—High signal, the reactor pressure has fallen to a value below these subsystems' maximum design pressure and a break inside the RCPB has occurred respectively. This Function also provides permissive for the closure of the recirculation discharge valves to ensure the LPCI subsystems inject into the proper RPV location. The Reactor Pressure—Low is one of the Functions assumed to be OPERABLE and capable of permitting initiation of the ECCS during the transients analyzed in References 1 and 3. In addition, the Reactor Pressure—Low Function is directly assumed in the analysis of the recirculation line break (Ref. 4). The core cooling function of the ECCS, along with the scram action of the RPS, ensures that the fuel peak cladding temperature remains below the limits of 10 CFR 50.46.

The Reactor Pressure—Low signals are initiated from four pressure transmitters that sense the reactor dome pressure.

The Allowable Value is low enough to prevent overpressuring the equipment in the low pressure ECCS, but high enough to ensure that the ECCS injection prevents the fuel peak cladding temperature from exceeding the limits of 10 CFR 50.46.

Four channels of Reactor Pressure—Low Function are only required to be OPERABLE when the ECCS is required to be OPERABLE to ensure that no single instrument failure can preclude ECCS initiation. Refer to LCO 3.5.1 and LCO 3.5.2 for Applicability Bases for the low pressure ECCS subsystems.

1.d, 2.g. Core Spray and Low Pressure Coolant Injection Pump Discharge Flow—Low (Bypass)

The minimum flow instruments are provided to protect the associated low pressure ECCS pump from overheating when the pump is operating and the associated injection valve is not fully open. The minimum flow line valve is opened when low flow is sensed, and the valve is automatically closed when the flow rate is adequate to protect the pump. The LPCI and

(continued)

BASES

APPLICABLE SAFETY ANALYSES LCO, and APPLICABILITY

1.d, 2.g. Core Spray and Low Pressure Coolant Injection Pump Discharge Flow—Low (Bypass) (continued)

CS Pump Discharge Flow—Low Functions are assumed to be OPERABLE and capable of closing the minimum flow valves to ensure that the low pressure ECCS flows assumed during the transients and accidents analyzed in References 1, 2, and 3 are met. The core cooling function of the ECCS, along with the scram action of the RPS, ensures that the fuel peak cladding temperature remains below the limits of 10 CFR 50.46.

One differential pressure switch per ECCS pump is used to detect the associated subsystems' flow rates. The logic is arranged such that each switch causes its associated minimum flow valve to open. The logic will close the minimum flow valve once the closure setpoint is exceeded. The LPCI minimum flow valves are time delayed such that the valves will not open for 10 seconds after the switches detect low flow. The time delay is provided to limit reactor vessel inventory loss during the startup of the RHR shutdown cooling mode. The Pump Discharge Flow—Low Allowable Values are high enough to ensure that the pump flow rate is sufficient to protect the pump, yet low enough to ensure that the closure of the minimum flow valve is initiated to allow full flow into the core.

Each channel of Pump Discharge Flow—Low Function (four CS channels and four LPCI channels) is only required to be OPERABLE when the associated ECCS is required to be OPERABLE to ensure that no single instrument failure can preclude the ECCS function. Refer to LCO 3.5.1 and LCO 3.5.2 for Applicability Bases for the low pressure ECCS subsystems.

1.e, 1.f. Core Spray Pump Start—Time Delay Relay

The purpose of this time delay is to stagger the start of the CS pumps that are in each of Divisions I and II to prevent overloading the power source. This Function is necessary when power is being supplied from the offsite sources or the standby power sources (DG). The CS Pump Start—Time Delay Relays are assumed to be OPERABLE in the accident and transient analyses requiring ECCS initiation. That is, the analyses assume that the pumps will initiate when required and excess loading will not cause failure of the power sources.

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

1.e, 1.f. Core Spray Pump Start—Time Delay Relay (continued)

There are eight Core Spray Pump Start—Time Delay Relays, two in each of the CS pump start logic circuits (one for when offsite power is available and one for when offsite power is not available). One of each type of time delay relay is dedicated to a single pump start logic, such that a single failure of a Core Spray Pump Start—Time Delay Relay will not result in the failure of more than one CS pump. In this condition, three of the four CS pumps will remain OPERABLE; thus, the single failure criterion is met (i.e., loss of one instrument does not preclude ECCS initiation). The Allowable Value for the Core Spray Pump Start—Time Delay Relays is chosen to be long enough so that the power source will not be overloaded and short enough so that ECCS operation is not degraded.

Each channel of Core Spray Pump Start—Time Delay Relay Function is required to be OPERABLE only when the associated CS subsystem is required to be OPERABLE. Refer to LCO 3.5.1 and LCO 3.5.2 for Applicability Bases for the CS subsystems.

2.d. Reactor Pressure—Low Low (Recirculation Discharge Valve Permissive)

Low reactor pressure signals are used as permissives for recirculation discharge valve closure. This ensures that the LPCI subsystems inject into the proper RPV location assumed in the safety analysis. The Reactor Pressure—Low Low is one of the Functions assumed to be OPERABLE and capable of closing the valve during the transients analyzed in References 1 and 3. The core cooling function of the ECCS, along with the scram action of the RPS, ensures that the fuel peak cladding temperature remains below the limits of 10 CFR 50.46. The Reactor Pressure—Low Low Function is directly assumed in the analysis of the recirculation line break (Ref. 4).

The Reactor Pressure—Low Low signals are initiated from four pressure transmitters that sense the reactor pressure.

The Allowable Value is chosen to ensure that the valves close prior to commencement of LPCI injection flow into the core, as assumed in the safety analysis.

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

2.d. Reactor Pressure—Low Low (Recirculation Discharge Valve Permissive) (continued)

Four channels of the Reactor Pressure—Low Low Function are only required to be OPERABLE in MODES 1, 2, and 3 with the associated recirculation pump discharge valve open. With the valve(s) closed, the function of the instrumentation has been performed; thus, the Function is not required. In MODES 4 and 5, the loop injection location is not critical since LPCI injection through the recirculation loop in either direction will still ensure that LPCI flow reaches the core (i.e., there is no significant reactor back pressure).

2.e. Reactor Vessel Shroud Level—Level 0

The Reactor Vessel Shroud Level—Level 0 Function is provided as a permissive to allow the RHR System to be manually aligned from the LPCI mode to the suppression pool cooling/spray or drywell spray modes. The reactor vessel shroud level permissive ensures that water in the vessel is approximately two thirds core height before the manual transfer is allowed. This ensures that LPCI is available to prevent or minimize fuel damage. This function may be overridden during accident conditions as allowed by plant procedures. Reactor Vessel Shroud Level—Level 0 Function is implicitly assumed in the analysis of the recirculation line break (Ref. 4) since the analysis assumes that no LPCI flow diversion occurs when reactor water level is below Level 0.

Reactor Vessel Shroud Level—Level 0 signals are initiated from two level transmitters that sense the difference between the pressure due to a constant column of water (reference leg) and the pressure due to the actual water level (variable leg) in the vessel. The Reactor Vessel Shroud Level—Level 0 Allowable Value is chosen to allow the low pressure core flooding systems to activate and provide adequate cooling before allowing a manual transfer.

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

2.e. Reactor Vessel Shroud Level—Level 0 (continued)

Two channels of the Reactor Vessel Shroud Level—Level 0 Function are only required to be OPERABLE in MODES 1, 2, and 3. In MODES 4 and 5, the specified initiation time of the LPCI subsystems is not assumed, and other administrative controls are adequate to control the valves associated with this Function (since the systems that the valves are opened for are not required to be OPERABLE in MODES 4 and 5 and are normally not used).

2.f. Low Pressure Coolant Injection Pump Start—Time Delay Relay

The purpose of this time delay is to stagger the start of the LPCI pumps that are in each of Divisions I and II, to prevent overloading the power source. This Function is only necessary when power is being supplied from offsite sources. The LPCI pumps start simultaneously with no time delay as soon as the standby source is available. The LPCI Pump Start—Time Delay Relays are assumed to be OPERABLE in the accident and transient analyses requiring ECCS initiation. That is, the analyses assume that the pumps will initiate when required and excess loading will not cause failure of the power sources.

There are eight LPCI Pump Start—Time Delay Relays, two in each of the RHR pump start logic circuits. Two time delay relays are dedicated to a single pump start logic. Both timers in the RHR pump start logic would have to fail to prevent an RHR pump from starting within the required time; therefore, the low pressure ECCS pumps will remain OPERABLE; thus, the single failure criterion is met (i.e., loss of one instrument does not preclude ECCS initiation). The Allowable Values for the LPCI Pump Start—Time Delay Relays are chosen to be long enough so that most of the starting transient of the first pump is complete before starting the second pump on the same 4 kV emergency bus and short enough so that ECCS operation is not degraded.

Each channel of LPCI Pump Start—Time Delay Relay Function is required to be OPERABLE only when the associated LPCI subsystem is required to be OPERABLE. Refer to LCO 3.5.1 and LCO 3.5.2 for Applicability Bases for the LPCI subsystems.

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

High Pressure Coolant Injection (HPCI) System

3.a. Reactor Vessel Water Level—Low Low (Level 2)

Low RPV water level indicates that the capability to cool the fuel may be threatened. Should RPV water level decrease too far, fuel damage could result. Therefore, the HPCI System is initiated at Level 2 to maintain level above the top of the active fuel. The Reactor Vessel Water Level—Low Low (Level 2) is one of the Functions assumed to be OPERABLE and capable of initiating HPCI during the transients analyzed in References 1 and 3. Additionally, the Reactor Vessel Water Level—Low Low (Level 2) Function associated with HPCI is credited as a backup to the Drywell Pressure—High Function for initiating HPCI in the analysis of the recirculation line break. The core cooling function of the ECCS, along with the scram action of the RPS, ensures that the fuel peak cladding temperature remains below the limits of 10 CFR 50.46.

Reactor Vessel Water Level—Low Low (Level 2) signals are initiated from four level transmitters that sense the difference between the pressure due to a constant column of water (reference leg) and the pressure due to the actual water level (variable leg) in the vessel.

The Reactor Vessel Water Level—Low Low (Level 2) Allowable Value is high enough such that for complete loss of feedwater flow, the Reactor Core Isolation Cooling (RCIC) System flow with HPCI assumed to fail will be sufficient to avoid initiation of low pressure ECCS at Reactor Vessel Water Level—Low Low Low (Level 1).

Four channels of Reactor Vessel Water Level—Low Low (Level 2) Function are required to be OPERABLE only when HPCI is required to be OPERABLE to ensure that no single instrument failure can preclude HPCI initiation. Refer to LCO 3.5.1 for HPCI Applicability Bases.

3.b. Drywell Pressure—High

High pressure in the drywell could indicate a break in the RCPB. The HPCI System is initiated upon receipt of the Drywell Pressure—High Function in order to minimize the possibility of fuel damage. The Drywell Pressure—High Function is directly assumed in the analysis of the

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

3.b. Drywell Pressure—High (continued)

recirculation line break (Ref. 4). The core cooling function of the ECCS, along with the scram action of the RPS, ensures that the fuel peak cladding temperature remains below the limits of 10 CFR 50.46.

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

Four channels of the Drywell Pressure—High Function are required to be OPERABLE when HPCI is required to be OPERABLE to ensure that no single instrument failure can preclude HPCI initiation. Refer to LCO 3.5.1 for the Applicability Bases for the HPCI System.

3.c. Reactor Vessel Water Level—High (Level 8)

High RPV water level indicates that sufficient cooling water inventory exists in the reactor vessel such that there is no danger to the fuel. Therefore, the Level 8 signal is used to trip the HPCI turbine to prevent overflow into the main steam lines (MSLs). The Reactor Vessel Water Level—High (Level 8) Function is assumed to trip the HPCI turbine in the feedwater controller failure transient analysis if HPCI is initiated.

Reactor Vessel Water Level—High (Level 8) signals for HPCI are initiated from two level transmitters from the wide range water level measurement instrumentation. Both Level 8 signals are required in order to trip the HPCI turbine. This ensures that no single instrument failure can preclude HPCI initiation. The Reactor Vessel Water Level—High (Level 8) Allowable Value is chosen to prevent flow from the HPCI System from overflowing into the MSLs.

Two channels of Reactor Vessel Water Level—High (Level 8) Function are required to be OPERABLE only when HPCI is required to be OPERABLE. Refer to LCO 3.5.1 and LCO 3.5.2 for HPCI Applicability Bases.

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

3.d. Condensate Storage Tank Level—Low

Low level in the CST indicates the unavailability of an adequate supply of makeup water from this normal source. Normally the suction valves between HPCI and the CST are open and, upon receiving a HPCI initiation signal, water for HPCI injection would be taken from the CST. However, if the water level in the CST falls below a preselected level, first the suppression pool suction valves automatically open, and then the CST suction valve automatically closes. This ensures that an adequate supply of makeup water is available to the HPCI pump. To prevent losing suction to the pump, the suction valves are interlocked so that the suppression pool suction valves must be open before the CST suction valve automatically closes. The Function is implicitly assumed in the accident and transient analyses (which take credit for HPCI) since the analyses assume that the HPCI suction source is the suppression pool.

Condensate Storage Tank Level—Low signals are initiated from two level switches. The logic is arranged such that either level switch can cause the suppression pool suction valves to open and the CST suction valve to close. The Condensate Storage Tank Level—Low Function Allowable Value is high enough to ensure adequate pump suction head while water is being taken from the CST.

Two channels of the Condensate Storage Tank Level—Low Function are required to be OPERABLE only when HPCI is required to be OPERABLE to ensure that no single instrument failure can preclude HPCI swap to suppression pool source. Refer to LCO 3.5.1 for HPCI Applicability Bases.

3.e. Suppression Pool Water Level—High

Excessively high suppression pool water could result in the loads on the suppression pool exceeding design values should there be a blowdown of the reactor vessel pressure through the safety/relief valves. Therefore, signals indicating high suppression pool water level are used to transfer the suction source of HPCI from the CST to the suppression pool to eliminate the possibility of HPCI continuing to provide additional water from a source outside containment. To prevent losing suction to the pump, the suction valves are interlocked so that the suppression pool suction valves must be open before the CST suction valve automatically closes.

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

3.e. Suppression Pool Water Level—High (continued)

This Function is implicitly assumed in the accident and transient analyses (which take credit for HPCI) since the analyses assume that the HPCI suction source is the suppression pool.

Suppression Pool Water Level—High signals are initiated from two level switches. The logic is arranged such that either switch can cause the suppression pool suction valves to open and the CST suction valve to close. The Allowable Value for the Suppression Pool Water Level—High Function is chosen to ensure that HPCI will be aligned for suction from the suppression pool to prevent HPCI from contributing to any further increase in the suppression pool level.

Two channels of Suppression Pool Water Level—High Function are required to be OPERABLE only when HPCI is required to be OPERABLE to ensure that no single instrument failure can preclude HPCI swap to suppression pool source. Refer to LCO 3.5.1 for HPCI Applicability Bases.

3.f. High Pressure Coolant Injection Pump Discharge Flow—Low (Bypass)

The minimum flow instrument is provided to protect the HPCI pump from overheating when the pump is operating at reduced flow. The minimum flow line valve is opened when low flow is sensed, and the valve is automatically closed when the flow rate is adequate to protect the pump. The High Pressure Coolant Injection Pump Discharge Flow—Low Function is assumed to be OPERABLE and capable of closing the minimum flow valve to ensure that the ECCS flow assumed during the transients analyzed in Reference 4 is met. The core cooling function of the ECCS, along with the scram action of the RPS, ensures that the fuel peak cladding temperature remains below the limits of 10 CFR 50.46.

One flow switch is used to detect the HPCI System's flow rate. The logic is arranged such that the transmitter causes the minimum flow valve to open. The logic will close the minimum flow valve once the closure setpoint is exceeded.

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

3.f. High Pressure Coolant Injection Pump Discharge Flow—Low (Bypass) (continued)

The High Pressure Coolant Injection Pump Discharge Flow—Low Allowable Value is high enough to ensure that pump flow rate is sufficient to protect the pump, yet low enough to ensure that the closure of the minimum flow valve is initiated to allow full flow into the core.

One channel is required to be OPERABLE when the HPCI is required to be OPERABLE. Refer to LCO 3.5.1 for HPCI Applicability Bases.

Automatic Depressurization System

4.a, 5.a. Reactor Vessel Water Level—Low Low Low (Level 1)

Low RPV water level indicates that the capability to cool the fuel may be threatened. Should RPV water level decrease too far, fuel damage could result. Therefore, ADS receives one of the signals necessary for initiation from this Function. The Reactor Vessel Water Level—Low Low Low (Level 1) is one of the Functions assumed to be OPERABLE and capable of initiating the ADS during the accident analyzed in Reference 4. The core cooling function of the ECCS, along with the scram action of the RPS, ensures that the fuel peak cladding temperature remains below the limits of 10 CFR 50.46.

Reactor Vessel Water Level—Low Low Low (Level 1) signals are initiated from four level transmitters that sense the difference between the pressure due to a constant column of water (reference leg) and the pressure due to the actual water level (variable leg) in the vessel. Four channels of Reactor Vessel Water Level—Low Low Low (Level 1) Function are required to be OPERABLE only when ADS is required to be OPERABLE to ensure that no single instrument failure can preclude ADS initiation. Two channels input to ADS trip system A, while the other two channels input to ADS trip system B. Refer to LCO 3.5.1 for ADS Applicability Bases.

The Reactor Vessel Water Level—Low Low Low (Level 1) Allowable Value is chosen to allow time for the low pressure core flooding systems to initiate and provide adequate cooling.

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

4.b, 5.b. Drywell Pressure—High

High pressure in the drywell could indicate a break in the RCPB. Therefore, ADS receives one of the signals necessary for initiation from this Function in order to minimize the possibility of fuel damage. The Drywell Pressure—High is assumed to be OPERABLE and capable of initiating the ADS during the accidents analyzed in Reference 4. The core cooling function of the ECCS, along with the scram action of the RPS, ensures that the fuel peak cladding temperature remains below the limits of 10 CFR 50.46.

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

Four channels of Drywell Pressure—High Function are only required to be OPERABLE when ADS is required to be OPERABLE to ensure that no single instrument failure can preclude ADS initiation. Two channels input to ADS trip system A, while the other two channels input to ADS trip system B. Refer to LCO 3.5.1 for ADS Applicability Bases.

4.c, 5.c. Automatic Depressurization System Initiation Timer

The purpose of the Automatic Depressurization System Initiation Timer is to delay depressurization of the reactor vessel to allow the HPCI System time to maintain reactor vessel water level. Since the rapid depressurization caused by ADS operation is one of the most severe transients on the reactor vessel, its occurrence should be limited. By delaying initiation of the ADS Function, the operator is given the chance to monitor the success or failure of the HPCI System to maintain water level, and then to decide whether or not to allow ADS to initiate, to delay initiation further by recycling the timer, or to inhibit initiation permanently. The Automatic Depressurization System Initiation Timer Function is assumed to be OPERABLE for the accident analysis of Reference 4 that requires ECCS initiation and assumes failure of the HPCI System.

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

4.c, 5.c. Automatic Depressurization System Initiation Timer (continued)

There are two Automatic Depressurization System Initiation Timer relays, one in each of the two ADS trip systems. The Allowable Value for the Automatic Depressurization System Initiation Timer is chosen so that there is still time after depressurization for the low pressure ECCS subsystems to provide adequate core cooling.

Two channels of the Automatic Depressurization System Initiation Timer Function are only required to be OPERABLE when the ADS is required to be OPERABLE to ensure that no single instrument failure can preclude ADS initiation. (One channel inputs to ADS trip system A, while the other channel inputs to ADS trip system B. Refer to LCO 3.5.1 for ADS Applicability Bases.

4.d, 5.d. Reactor Vessel Water Level— Low Low Low (Level 1) (Permissive)

Low reactor water level signals are used as permissives in the ADS trip systems. This ensures after a high drywell pressure signal or a low reactor water level signal (Level 1) is received and the timer times out that a low reactor water level (Level 1), signal is present to allow the ADS initiation (after a confirmatory Level 4 signal, see Bases for Functions 4.e, 5.e, Reactor Vessel Water Confirmatory Level—Low (Level 4).

Reactor Vessel Water Level—Low Low Low (Level 1), signals are initiated from four level transmitters that sense the difference between the pressure due to a constant column of water (reference leg) and the pressure doe to the actual water level (variable leg) in the vessel. The Reactor Vessel Water Level—Low Low Low (Level 1) Allowable Value is chosen to allow time for the low pressure core flooding system to initiate and provide adequate cooling.

Four channels of the Reactor Vessel Water Level—Low Low Low (Level 1) Function are required to be OPERABLE to ensure that no single instrument failure can preclude ADS initiation. Two channels input to ADS trip system A while the other two channels input to ADS trip system B. Refer to LCO 3.5.1 for ADS Applicability Bases.

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

4.e, 5.e. Reactor Vessel Water Confirmatory Level—Low (Level 4)

The Reactor Vessel Water Confirmatory Level—Low (Level 4) Function is used by the ADS only as a confirmatory low water level signal. ADS receives one of the signals necessary for initiation from Reactor Vessel Water Level—Low Low Low (Level 1) signals. In order to prevent spurious initiation of the ADS due to spurious Level 1 signals, a Level 4 signal must also be received before ADS initiation commences.

Reactor Vessel Water Confirmatory Level—Low (Level 4) signals are initiated from two level transmitters that sense the difference between the pressure due to a constant column of water (reference leg) and the pressure due to the actual water level (variable leg) in the vessel. The Allowable Value for Reactor Vessel Water Confirmatory Level—Low (Level 4) is selected to be above the RPS Level 3 scram Allowable Value for convenience.

Two channels of Reactor Vessel Water Confirmatory Level—Low (Level 4) Function are only required to be OPERABLE when the ADS is required to be OPERABLE to ensure that no single instrument failure can preclude ADS initiation. One channel inputs to ADS trip system A, while the other channel inputs to ADS trip system B. Refer to LCO 3.5.1 for ADS Applicability Bases.

4.f, 4.g, 5.f, 5.g. Core Spray and Low Pressure Coolant Injection Pump Discharge Pressure—High

The Pump Discharge Pressure—High signals from the CS and LPCI pumps are used as permissives for ADS initiation, indicating that there is a source of low pressure cooling water available once the ADS has depressurized the vessel. Pump Discharge Pressure—High is one of the Functions assumed to be OPERABLE and capable of permitting ADS initiation during the events analyzed in Reference 4 with an assumed HPCI failure. For these events the ADS depressurizes the reactor vessel so that the low pressure ECCS can perform the core cooling functions. This core cooling function of the ECCS, along with the scram action of the RPS, ensures that the fuel peak cladding temperature remains below the limits of 10 CFR 50.46.

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

4.f, 4.g, 5.f, 5.g. Core Spray and Low Pressure Coolant Injection Pump Discharge Pressure—High (continued)

Pump discharge pressure signals are initiated from twelve pressure transmitters, two on the discharge side of each of the four LPCI pumps and one on the discharge side of each CS pump. There are two ADS low pressure ECCS pump permissives in each trip system. Each of the permissives receives inputs from all four LPCI pumps (different signals for each permissive) and two CS pumps, one from each subsystem (different pumps for each permissive). In order to generate an ADS permissive in one trip system, it is necessary that only one LPCI pump or two CS pumps in proper combination (C or D and A or B) indicate the high discharge pressure condition in each of the two permissives. The Pump Discharge Pressure—High Allowable Value is less than the pump discharge pressure when the pump is operating in a full flow mode and high enough to avoid any condition that results in a discharge pressure permissive when the CS and LPCI pumps are aligned for injection and the pumps are not running. The actual operating point of this function is not assumed in any transient or accident analysis. However, this Function is indirectly assumed to operate (in Reference 4) to provide the ADS permissive to depressurize the RCS to allow the ECCS low pressure systems to operate.

Twelve channels of Core Spray and Low Pressure Coolant Injection Pump Discharge Pressure—High Function are only required to be OPERABLE when the ADS is required to be OPERABLE to ensure that no single instrument failure can preclude ADS initiation. Four CS channels associated with CS pumps A through D and eight LPCI channels associated with LPCI pumps A through D are required for both trip systems. Refer to LCO 3.5.1 for ADS Applicability Bases.

4.h, 5.h. Automatic Depressurization System Low Water Level Actuation Timer

One of the signals required for ADS initiation is Drywell Pressure—High. However, if the event requiring ADS initiation occurs outside the drywell (e.g., main steam line break outside containment), a high drywell pressure signal may never be present. Therefore, the Automatic Depressurization System Low Water Level Actuation Timer is used to bypass the Drywell Pressure—High Function after a

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

4.h, 5.h. Automatic Depressurization System Low Water Level Actuation Timer (continued)

certain time period has elapsed. Operation of the Automatic Depressurization System Low Water Level Actuation Timer Function is assumed in the accident analysis of Reference 4 that requires ECCS initiation and assumes failure of the HPCI system.

There are four Automatic Depressurization System Low Water Level Actuation Timer relays, two in each of the two ADS trip systems. The Allowable Value for the Automatic Depressurization System Low Water Level Actuation Timer is chosen to ensure that there is still time after depressurization for the low pressure ECCS subsystems to provide adequate core cooling.

Four channels of the Automatic Depressurization System Low Water Level Actuation Timer Function are only required to be OPERABLE when the ADS is required to be OPERABLE to ensure that no single instrument failure can preclude ADS initiation. Refer to LCO 3.5.1 for ADS Applicability Bases.

ACTIONS

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

A.1

Required Action A.1 directs entry into the appropriate Condition referenced in Table 3.3.5.1-1. The applicable Condition referenced in the table is Function dependent. Each time a channel is discovered inoperable, Condition A is entered for that channel and provides for transfer to the appropriate subsequent Condition.

(continued)

BASES

ACTIONS (continued)

B.1, B.2, and B.3

Required Actions B.1 and B.2 are intended to ensure that appropriate actions are taken if multiple, inoperable, untripped channels within the same Function result in redundant automatic initiation capability being lost for the feature(s). Required Action B.1 features would be those that are initiated by Functions 1.a, 1.b, 2.a, and 2.b (e.g., low pressure ECCS). The Required Action B.2 system would be HPCI. For Required Action B.1, redundant automatic initiation capability is lost if (a) two or more Function 1.a channels are inoperable and untripped such that both trip systems lose initiation capability, (b) two or more Function 2.a channels are inoperable and untripped such that both trip systems lose initiation capability, (c) two or more Function 1.b channels are inoperable and untripped such that both trip systems lose initiation capability, or (d) two or more Function 2.b channels are inoperable and untripped such that both trip systems lose initiation capability. For low pressure ECCS, since each inoperable channel would have Required Action B.1 applied separately (refer to ACTIONS Note), each inoperable channel would only require the affected portion of the associated system of low pressure ECCS and DGs to be declared inoperable. However, since channels in both associated low pressure ECCS subsystems (e.g., both CS subsystems) are inoperable and untripped, and the Completion Times started concurrently for the channels in both subsystems, this results in the affected portions in the associated low pressure ECCS and DGs being concurrently declared inoperable.

For Required Action B.2, redundant automatic HPCI initiation capability is lost if two or more Function 3.a or two Function 3.b channels are inoperable and untripped such that the trip system loses initiation capability. In this situation (loss of redundant automatic initiation capability), the 24 hour allowance of Required Action B.3 is not appropriate and the HPCI System must be declared inoperable within 1 hour. As noted (Note 1 to Required Action B.1), Required Action B.1 is only applicable in MODES 1, 2, and 3. In MODES 4 and 5, the specific initiation time of the low pressure ECCS is not assumed and the probability of a LOCA is lower. Thus, a total loss of

(continued)

BASES

ACTIONS

B.1, B.2, and B.3 (continued)

initiation capability for 24 hours (as allowed by Required Action B.3) is allowed during MODES 4 and 5. There is no similar Note provided for Required Action B.2 since HPCI instrumentation is not required in MODES 4 and 5; thus, a Note is not necessary.

Notes are also provided (Note 2 to Required Action B.1 and the Note to Required Action B.2) to delineate which Required Action is applicable for each Function that requires entry into Condition B if an associated channel is inoperable. This ensures that the proper loss of initiation capability check is performed. Required Action B.1 (the Required Action for certain inoperable channels in the low pressure ECCS subsystems) is not applicable to Function 2.e, since this Function provides backup to administrative controls ensuring that operators do not divert LPCI flow from injecting into the core when needed. Thus, a total loss of Function 2.e capability for 24 hours is allowed, since the LPCI subsystems remain capable of performing their intended function.

The Completion Time is intended to allow the operator time to evaluate and repair any discovered inoperabilities. This Completion Time also allows for an exception to the normal "time zero" for beginning the allowed outage time "clock." For Required Action B.1, the Completion Time only begins upon discovery that a redundant feature in the same system (e.g., both CS subsystems) cannot be automatically initiated due to inoperable, untripped channels within the same Function as described in the paragraph above. For Required Action B.2, the Completion Time only begins upon discovery that the HPCI System cannot be automatically initiated due to two inoperable, untripped channels for the associated Function in the same trip system. The 1 hour Completion Time from discovery of loss of initiation capability is acceptable because it minimizes risk while allowing time for restoration or tripping of channels.

Because of the diversity of sensors available to provide initiation signals and the redundancy of the ECCS design, an allowable out of service time of 24 hours has been shown to be acceptable (Ref. 5) to permit restoration of any inoperable channel to OPERABLE status. If the inoperable channel cannot be restored to OPERABLE status within the

(continued)

BASES

ACTIONS

B.1, B.2, and B.3 (continued)

allowable out of service time, the channel must be placed in the tripped condition per Required Action B.3. Placing the inoperable channel in trip would conservatively compensate for the inoperability, restore capability to accommodate a single failure, and allow operation to continue. Alternately, if it is not desired to place the channel in trip (e.g., as in the case where placing the inoperable channel in trip would result in an initiation), Condition H must be entered and its Required Action taken.

C.1 and C.2

Required Action C.1 is intended to ensure that appropriate actions are taken if multiple, inoperable channels within the same Function result in redundant automatic initiation capability being lost for the feature(s). Required Action C.1 features would be those that are initiated by Functions 1.c, 1.e, 1.f, 2.c, 2.d, and 2.f (i.e., low pressure ECCS). Redundant automatic initiation capability is lost if either (a) two or more Function 1.c channels are inoperable in the same trip system such that the trip system loses initiation capability, (b) two or more Function 1.e channels are inoperable affecting CS pumps in different subsystems, (c) two or more Function 1.f channels are inoperable affecting CS pumps in different subsystems, (d) two or more Function 2.c channels are inoperable in the same trip system such that the trip system loses initiation capability, (e) two or more Function 2.d channels are inoperable in the same trip system such that the trip system loses initiation capability, or (f) three or more Function 2.f channels are inoperable. In this situation (loss of redundant automatic initiation capability), the 24 hour allowance of Required Action C.2 is not appropriate and the feature(s) associated with the inoperable channels must be declared inoperable within 1 hour. Since each inoperable channel would have Required Action C.1 applied separately (refer to ACTIONS Note), each inoperable channel would only require the affected portion of the associated system to be declared inoperable. However, since channels for both low pressure ECCS subsystems are inoperable (e.g., both CS subsystems), and the Completion Times started concurrently for the channels in both subsystems, this results in the affected portions in both subsystems being

(continued)

BASES

ACTIONS

C.1 and C.2 (continued)

concurrently declared inoperable. For Functions 1.c, 1.e, 1.f, 2.c, 2.d, and 2.f, the affected portions are the associated low pressure ECCS pumps. As noted (Note 1), Required Action C.1 is only applicable in MODES 1, 2, and 3. In MODES 4 and 5, the specific initiation time of the ECCS is not assumed and the probability of a LOCA is lower. Thus, a total loss of automatic initiation capability for 24 hours (as allowed by Required Action C.2) is allowed during MODES 4 and 5.

Note 2 states that Required Action C.1 is only applicable for Functions 1.c, 1.e, 1.f, 2.c, 2.d, and 2.f. Required Action C.1 is not applicable to Function 3.c (which also requires entry into this Condition if a channel in this Function is inoperable), since the loss of one channel results in a loss of the Function (two-out-of-two logic). This loss was considered during the development of Reference 5 and considered acceptable for the 24 hours allowed by Required Action C.2.

The Completion Time is intended to allow the operator time to evaluate and repair any discovered inoperabilities. This Completion Time also allows for an exception to the normal "time zero" for beginning the allowed outage time "clock." For Required Action C.1, the Completion Time only begins upon discovery that the same feature in both subsystems (e.g., both CS subsystems) cannot be automatically initiated due to inoperable channels within the same Function as described in the paragraph above. The 1 hour Completion Time from discovery of loss of initiation capability is acceptable because it minimizes risk while allowing time for restoration of channels.

Because of the diversity of sensors available to provide initiation signals and the redundancy of the ECCS design, an allowable out of service time of 24 hours has been shown to be acceptable (Ref. 5) to permit restoration of any inoperable channel to OPERABLE status. If the inoperable channel cannot be restored to OPERABLE status within the allowable out of service time, Condition H must be entered and its Required Action taken. The Required Actions do not allow placing the channel in trip since this action would either cause the initiation or it would not necessarily result in a safe state for the channel in all events.

(continued)

BASES

ACTIONS (continued)

D.1, D.2.1, and D.2.2

Required Action D.1 is intended to ensure that appropriate actions are taken if multiple, inoperable, untripped channels within the same Function result in a complete loss of automatic component initiation capability for the HPCI System. Automatic component initiation capability is lost if two Function 3.d channels or two Function 3.e channels are inoperable and untripped. In this situation (loss of automatic suction swap), the 24 hour allowance of Required Actions D.2.1 and D.2.2 is not appropriate and the HPCI System must be declared inoperable within 1 hour after discovery of loss of HPCI initiation capability. As noted, Required Action D.1 is only applicable if the HPCI pump suction is not aligned to the suppression pool, since, if aligned, the Function is already performed.

The Completion Time is intended to allow the operator time to evaluate and repair any discovered inoperabilities. This Completion Time also allows for an exception to the normal "time zero" for beginning the allowed outage time "clock." For Required Action D.1, the Completion Time only begins upon discovery that the HPCI System cannot be automatically aligned to the suppression pool due to two inoperable, untripped channels in the same Function. The 1 hour Completion Time from discovery of loss of initiation capability is acceptable because it minimizes risk while allowing time for restoration or tripping of channels.

Because of the diversity of sensors available to provide initiation signals and the redundancy of the ECCS design, an allowable out of service time of 24 hours has been shown to be acceptable (Ref. 5) to permit restoration of any inoperable channel to OPERABLE status. If the inoperable channel cannot be restored to OPERABLE status within the allowable out of service time, the channel must be placed in the tripped condition per Required Action D.2.1 or the suction source must be aligned to the suppression pool per Required Action D.2.2. Placing the inoperable channel in trip performs the intended function of the channel (shifting the suction source to the suppression pool). Performance of either of these two Required Actions will allow operation to continue. If Required Action D.2.1 or D.2.2 is performed, measures should be taken to ensure that the HPCI System

(continued)

BASES

ACTIONS

D.1, D.2.1, and D.2.2 (continued)

piping remains filled with water. Alternately, if it is not desired to perform Required Actions D.2.1 and D.2.2 (e.g., as in the case where shifting the suction source could drain down the HPCI suction piping), Condition H must be entered and its Required Action taken.

E.1 and E.2

Required Action E.1 is intended to ensure that appropriate actions are taken if multiple, inoperable channels within the Core Spray and Low Pressure Coolant Injection Pump, Discharge Flow - Low (Bypass) Functions result in redundant automatic initiation capability being lost for the feature(s). For Required Action E.1, the features would be those that are initiated by Functions 1.d and 2.g (e.g., low pressure ECCS). Redundant automatic initiation capability is lost if (a) two or more Function 1.d channels are inoperable affecting CS pumps in different subsystems or (b) three or more Function 2.g channels are inoperable. Since each inoperable channel would have Required Action E.1 applied separately (refer to ACTIONS Note), each inoperable channel would only require the affected low pressure ECCS pump to be declared inoperable. However, since channels for more than one low pressure ECCS pump are inoperable, and the Completion Times started concurrently for the channels of the low pressure ECCS pumps, this results in the affected low pressure ECCS pumps being concurrently declared inoperable.

In this situation (loss of redundant automatic initiation capability), the 7 day allowance of Required Action E.2 is not appropriate and the subsystem associated with each inoperable channel must be declared inoperable within 1 hour. As noted (Note 1 to Required Action E.1), Required Action E.1 is only applicable in MODES 1, 2, and 3. In MODES 4 and 5, the specific initiation time of the ECCS is not assumed and the probability of a LOCA is lower. Thus, a total loss of initiation capability for 7 days (as allowed by Required Action E.2) is allowed during MODES 4 and 5. A Note is also provided (Note 2 to Required Action E.1) to delineate that Required Action E.1 is only applicable to low

(continued)

BASES

ACTIONS

E.1 and E.2 (continued)

pressure ECCS Functions. Required Action E.1 is not applicable to HPCI Function 3.f since the loss of one channel results in a loss of function (one-out-of-one logic). This loss was considered during the development of Reference 5 and considered acceptable for the 7 days allowed by Required Action E.2.

The Completion Time is intended to allow the operator time to evaluate and repair any discovered inoperabilities. This Completion Time also allows for an exception to the normal "time zero" for beginning the allowed outage time "clock."

For Required Action E.1, the Completion Time only begins upon discovery that a redundant feature in the same system (e.g., both CS subsystems) cannot be automatically initiated due to inoperable channels within the same Function as described in the paragraph above. The 1 hour Completion Time from discovery of loss of initiation capability is acceptable because it minimizes risk while allowing time for restoration of channels.

If the instrumentation that controls the pump minimum flow valve is inoperable, such that the valve will not automatically open, extended pump operation with no injection path available could lead to pump overheating and failure. If there were a failure of the instrumentation, such that the valve would not automatically close, a portion of the pump flow could be diverted from the reactor vessel injection path, causing insufficient core cooling. These consequences can be averted by the operator's manual control of the valve, which would be adequate to maintain ECCS pump protection and required flow. Furthermore, other ECCS pumps would be sufficient to complete the assumed safety function if no additional single failure were to occur. The 7 day Completion Time of Required Action E.2 to restore the inoperable channel to OPERABLE status is reasonable based on the remaining capability of the associated ECCS subsystems, the redundancy available in the ECCS design, and the low probability of a DBA occurring during the allowed out of service time. If the inoperable channel cannot be restored to OPERABLE status within the allowable out of service time, Condition H must be entered and its Required Action taken. The Required Actions do not allow placing the channel in trip since this action would not necessarily result in a safe state for the channel in all events.

(continued)

BASES

ACTIONS (continued)

F.1 and F.2

Required Action F.1 is intended to ensure that appropriate actions are taken if multiple, inoperable, untripped channels within similar ADS trip system A and B Functions result in redundant automatic initiation capability being lost for the ADS. Redundant automatic initiation capability is lost if either (a) one or more Function 4.a channel and one or more Function 5.a channel are inoperable and untripped, (b) one or more Function 4.b channel and one or more Function 5.b channel are inoperable and untripped, (c) one or more Function 4.d channel and one or more Function 5.d channel are inoperable and untripped, or (d) one Function 4.e channel and one Function 5.e channel are inoperable and untripped.

In this situation (loss of automatic initiation capability), the 96 hour or 8 day allowance, as applicable, of Required Action F.2 is not appropriate and all ADS valves must be declared inoperable within 1 hour after discovery of loss of ADS initiation capability.

The Completion Time is intended to allow the operator time to evaluate and repair any discovered inoperabilities. This Completion Time also allows for an exception to the normal "time zero" for beginning the allowed outage time "clock." For Required Action F.1, the Completion Time only begins upon discovery that the ADS cannot be automatically initiated due to inoperable, untripped channels within similar ADS trip system Functions as described in the paragraph above. The 1 hour Completion Time from discovery of loss of initiation capability is acceptable because it minimizes risk while allowing time for restoration or tripping of channels.

Because of the diversity of sensors available to provide initiation signals and the redundancy of the ECCS design, an allowable out of service time of 8 days has been shown to be acceptable (Ref. 5) to permit restoration of any inoperable channel to OPERABLE status if both HPCI and RCIC are OPERABLE. If either HPCI or RCIC is inoperable, the time is shortened to 96 hours. If the status of HPCI or RCIC changes such that the Completion Time changes from 8 days to 96 hours, the 96 hours begins upon discovery of HPCI or RCIC inoperability. However, the total time for an inoperable, untripped channel cannot exceed 8 days. If the status of

(continued)

BASES

ACTIONS

F.1 and F.2 (continued)

HPCI or RCIC changes such that the Completion Time changes from 96 hours to 8 days, the "time zero" for beginning the 8 day "clock" begins upon discovery of the inoperable, untripped channel. If the inoperable channel cannot be restored to OPERABLE status within the allowable out of service time, the channel must be placed in the tripped condition per Required Action F.2. Placing the inoperable channel in trip would conservatively compensate for the inoperability, restore capability to accommodate a single failure, and allow operation to continue. Alternately, if it is not desired to place the channel in trip (e.g., as in the case where placing the inoperable channel in trip would result in an initiation), Condition H must be entered and its Required Action taken.

G.1 and G.2

Required Action G.1 is intended to ensure that appropriate actions are taken if multiple, inoperable channels within similar ADS trip system Functions result in automatic initiation capability being lost for the ADS. Automatic initiation capability is lost if either (a) one Function 4.c channel and one Function 5.c channel are inoperable, (b) a combination of Function 4.f, 4.g, 5.f, and 5.g channels are inoperable such that channels associated with five or more low pressure ECCS pumps are inoperable, or (c) one or more Function 4.h channels and one or more Function 5.h channels are inoperable.

In this situation (loss of automatic initiation capability), the 96 hour or 8 day allowance, as applicable, of Required Action G.2 is not appropriate, and all ADS valves must be declared inoperable within 1 hour after discovery of loss of ADS initiation capability. The Note to Required Action G.1 states that Required Action G.1 is only applicable for Functions 4.c, 4.f, 4.g, 4.h, 5.c, 5.f, 5.g, and 5.h.

The Completion Time is intended to allow the operator time to evaluate and repair any discovered inoperabilities. This Completion Time also allows for an exception to the normal "time zero" for beginning the allowed outage time "clock." For Required Action G.1, the Completion Time only begins

(continued)

BASES

ACTIONS

G.1 and G.2 (continued)

upon discovery that the ADS cannot be automatically initiated due to inoperable channels within similar ADS trip system Functions as described in the paragraph above. The 1 hour Completion Time from discovery of loss of initiation capability is acceptable because it minimizes risk while allowing time for restoration or tripping of channels.

Because of the diversity of sensors available to provide initiation signals and the redundancy of the ECCS design, an allowable out of service time of 8 days has been shown to be acceptable (Ref. 5) to permit restoration of any inoperable channel to OPERABLE status if both HPCI and RCIC are OPERABLE (Required Action G.2). If either HPCI or RCIC is inoperable, the time shortens to 96 hours. If the status of HPCI or RCIC changes such that the Completion Time changes from 8 days to 96 hours, the 96 hours begins upon discovery of HPCI or RCIC inoperability. However, the total time for an inoperable channel cannot exceed 8 days. If the status of HPCI or RCIC changes such that the Completion Time changes from 96 hours to 8 days, the "time zero" for beginning the 8 day "clock" begins upon discovery of the inoperable channel. If the inoperable channel cannot be restored to OPERABLE status within the allowable out of service time, Condition H must be entered and its Required Action taken. The Required Actions do not allow placing the channel in trip since this action would not necessarily result in a safe state for the channel in all events.

H.1

With any Required Action and associated Completion Time not met, the associated feature(s) may be incapable of performing the intended function, and the supported feature(s) associated with inoperable untripped channels must be declared inoperable immediately.

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS

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

The Surveillances are modified by a Note to indicate that when a channel is placed in an inoperable status solely for performance of required Surveillances, entry into associated Conditions and Required Actions may be delayed for up to 6 hours as follows: (a) for Functions 3.c and 3.f; and (b) for Functions other than 3.c and 3.f provided the associated Function or the redundant Function maintains ECCS initiation capability. Upon completion of the Surveillance, or expiration of the 6 hour allowance, the channel must be returned to OPERABLE status or the applicable Condition entered and Required Actions taken. This Note is based on the reliability analysis (Ref. 5) assumption of the average time required to perform channel surveillance. That analysis demonstrated that the 6 hour testing allowance does not significantly reduce the probability that the ECCS will initiate when necessary.

SR 3.3.5.1.1

Performance of the CHANNEL CHECK once every 12 hours ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the parameter indicated on one channel to a similar parameter on other channels. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value. Significant deviations between the instrument channels could be an indication of excessive instrument drift in one of the channels or something even more serious. A CHANNEL CHECK guarantees that undetected outright channel failure is limited to 12 hours; thus, it is key to verifying the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

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

(continued)

BASES

SURVEILLANCE REQUIREMENTS

SR 3.3.5.1.1 (continued)

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

SR 3.3.5.1.2

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

The Frequency of 92 days is based on the reliability analyses of Reference 5.

SR 3.3.5.1.3 and SR 3.3.5.1.4

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

The 92 day Frequency of SR 3.3.5.1.3 is conservative with respect to the magnitude of equipment drift assumed in the setpoint analysis.

The Frequency of SR 3.3.5.1.4 is based upon the assumption of a 24 month calibration interval in the determination of the magnitude of equipment drift in the setpoint analysis.

(continued)

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.5.1.5

The LOGIC SYSTEM FUNCTIONAL TEST demonstrates the OPERABILITY of the required initiation logic for a specific channel. The system functional testing performed in LCO 3.5.1, LCO 3.5.2, LCO 3.8.1, and LCO 3.8.2 overlaps this Surveillance to complete testing of the assumed safety function.

While this Surveillance can be performed with the reactor at power for some of the Functions, operating experience has shown that these components will pass the Surveillance when performed at the 24 month Frequency. Therefore, the Frequency was found to be acceptable from a reliability standpoint.

REFERENCES

1. UFSAR, Section 6.5.

2. UFSAR, Section 7.4.

3. UFSAR, Chapter 14.

4. NEDC-32163-P, "Peach Bottom Atomic Power Station Units 2 and 3, SAFER/GESTR-LOCA, Loss-of-Coolant Accident Analysis," January 1993.

5. NEDC-30936-P-A, "BWR Owners' Group Technical Specification Improvement Analyses for ECCS Actuation Instrumentation, Part 2," December 1988.

B 3.3 INSTRUMENTATION

B 3.3.5.2 Reactor Core Isolation Cooling (RCIC) System Instrumentation

BASES

BACKGROUND

The purpose of the RCIC System instrumentation is to initiate actions to ensure adequate core cooling when the reactor vessel is isolated from its primary heat sink (the main condenser) and normal coolant makeup flow from the Reactor Feedwater System is insufficient or unavailable, such that RCIC System initiation occurs and maintains sufficient reactor water level such that an initiation of the low pressure Emergency Core Cooling Systems (ECCS) pumps does not occur. A more complete discussion of RCIC System operation is provided in the Bases of LCO 3.5.3, "RCIC System."

The RCIC System may be initiated by automatic means. Automatic initiation occurs for conditions of Reactor Vessel Water Level—Low Low (Level 2). The variable is monitored by four transmitters that are connected to four pressure compensation instruments. The outputs of the pressure compensation instruments are connected to relays whose contacts are arranged in a one-out-of-two taken twice logic arrangement. Once initiated, the RCIC logic seals in and can be reset by the operator only when the reactor vessel water level signals have cleared.

The RCIC test line isolation valve is closed on a RCIC initiation signal to allow full system flow and maintain primary containment isolated in the event RCIC is not operating.

The RCIC System also monitors the water level in the condensate storage tank (CST) since this is the initial source of water for RCIC operation. Reactor grade water in the CST is the normal source. Upon receipt of a RCIC initiation signal, the CST suction valve is automatically signaled to open (it is normally in the open position) unless the pump suction from the suppression pool valves is open. If the water level in the CST falls below a preselected level, first the suppression pool suction valves automatically open, and then the CST suction valve automatically closes. Two level switches are used to detect low water level in the CST. Either switch can cause the suppression pool suction valves to open. The opening of the

(continued)

BASES

BACKGROUND (continued)

suppression pool suction valves causes the CST suction valve to close. This prevents losing suction to the pump when automatically transferring suction from the CST to the suppression pool on low CST level.

The RCIC System provides makeup water to the reactor until the reactor vessel water level reaches the high water level (Level 8) setting (two-out-of-two logic), at which time the RCIC steam supply valve closes. The RCIC System restarts if vessel level again drops to the low level initiation point (Level 2).

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

The function of the RCIC System is to respond to transient events by producing makeup coolant to the reactor. The RCIC System is not an Engineered Safeguard System and no credit is taken in the safety analyses for RCIC System operation. Based on its contribution to the reduction of overall plant risk, however, the system, and therefore its instrumentation meets Criterion 4 of NRC Policy Statement.

The OPERABILITY of the RCIC System instrumentation is dependent upon the OPERABILITY of the individual instrumentation channel Functions specified in Table 3.3.5.2-1. Each Function must have a required number of OPERABLE channels with their setpoints within the specified Allowable Values, where appropriate. A channel is inoperable if its actual trip setting is not within its required Allowable Value. The actual setpoint is calibrated consistent with applicable setpoint methodology assumptions.

Allowable Values are specified for each RCIC System instrumentation Function specified in the Table. Trip setpoints are specified in the setpoint calculations. The setpoints are selected to ensure that the settings do not exceed the Allowable Value between CHANNEL CALIBRATIONS. Operation with a trip setting less conservative than the trip setpoint, but within its Allowable Value, is acceptable. Each Allowable Value specified accounts for instrument uncertainties appropriate to the Function. These uncertainties are described in the setpoint methodology.

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

The individual Functions are required to be OPERABLE in MODE 1, and in MODES 2 and 3 with reactor steam dome pressure > 150 psig since this is when RCIC is required to be OPERABLE. (Refer to LCO 3.5.3 for Applicability Bases for the RCIC System.)

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

1. Reactor Vessel Water Level—Low Low (Level 2)

Low reactor pressure vessel (RPV) water level indicates that normal feedwater flow is insufficient to maintain reactor vessel water level and that the capability to cool the fuel may be threatened. Should RPV water level decrease too far, fuel damage could result. Therefore, the RCIC System is initiated at Level 2 to assist in maintaining water level above the top of the active fuel.

Reactor Vessel Water Level—Low Low (Level 2) signals are initiated from four level transmitters that sense the difference between the pressure due to a constant column of water (reference leg) and the pressure due to the actual water level (variable leg) in the vessel.

The Reactor Vessel Water Level—Low Low (Level 2) Allowable Value is set high enough such that for complete loss of feedwater flow, the RCIC System flow with high pressure coolant injection assumed to fail will be sufficient to avoid initiation of low pressure ECCS at Level 1.

Four channels of Reactor Vessel Water Level—Low Low (Level 2) Function are available and are required to be OPERABLE when RCIC is required to be OPERABLE to ensure that no single instrument failure can preclude RCIC initiation. Refer to LCO 3.5.3 for RCIC Applicability Bases.

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

2. Reactor Vessel Water Level—High (Level 8)

High RPV water level indicates that sufficient cooling water inventory exists in the reactor vessel such that there is no danger to the fuel. Therefore, the Level 8 signal is used to close the RCIC steam supply valve to prevent overflow into the main steam lines (MSLs).

Reactor Vessel Water Level—High (Level 8) signals for RCIC are initiated from four level transmitters, which sense the difference between the pressure due to a constant column of water (reference leg) and the pressure due to the actual water level (variable leg) in the vessel. These four level transmitters are connected to two pressure compensation instruments (channels).

The Reactor Vessel Water Level—High (Level 8) Allowable Value is high enough to preclude isolating the injection valve of the RCIC during normal operation, yet low enough to trip the RCIC System prior to water overflowing into the MSLs.

Two channels of Reactor Vessel Water Level—High (Level 8) Function are available and are required to be OPERABLE when RCIC is required to be OPERABLE to ensure that no single instrument failure can preclude RCIC initiation. Refer to LCO 3.5.3 for RCIC Applicability Bases.

3. Condensate Storage Tank Level—Low

Low level in the CST indicates the unavailability of an adequate supply of makeup water from this normal source. Normally, the suction valve between the RCIC pump and the CST is open and, upon receiving a RCIC initiation signal, water for RCIC injection would be taken from the CST. However, if the water level in the CST falls below a preselected level, first the suppression pool suction valves automatically open, and then the CST suction valve automatically closes. This ensures that an adequate supply of makeup water is available to the RCIC pump. To prevent losing suction to the pump, the suction valves are interlocked so that the suppression pool suction valves must be open before the CST suction valve automatically closes.

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

3. Condensate Storage Tank Level—Low (continued)

Two level switches are used to detect low water level in the CST. The Condensate Storage Tank Level—Low Function Allowable Value is set high enough to ensure adequate pump suction head while water is being taken from the CST.

Two channels of the CST Level—Low Function are available and are required to be OPERABLE when RCIC is required to be OPERABLE to ensure that no single instrument failure can preclude RCIC swap to suppression pool source. Refer to LCO 3.5.3 for RCIC Applicability Bases.

ACTIONS

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

A.1

Required Action A.1 directs entry into the appropriate Condition referenced in Table 3.3.5.2-1. The applicable Condition referenced in the Table is Function dependent. Each time a channel is discovered to be inoperable, Condition A is entered for that channel and provides for transfer to the appropriate subsequent Condition.

(continued)

BASES

ACTIONS (continued)

B.1 and B.2

Required Action B.1 is intended to ensure that appropriate actions are taken if multiple, inoperable, untripped channels within the same Function result in a complete loss of automatic initiation capability for the RCIC System. In this case, automatic initiation capability is lost if two Function 1 channels in the same trip system are inoperable and untripped. In this situation (loss of automatic initiation capability), the 24 hour allowance of Required Action B.2 is not appropriate, and the RCIC System must be declared inoperable within 1 hour after discovery of loss of RCIC initiation capability.

The Completion Time is intended to allow the operator time to evaluate and repair any discovered inoperabilities. This Completion Time also allows for an exception to the normal "time zero" for beginning the allowed outage time "clock." For Required Action B.1, the Completion Time only begins upon discovery that the RCIC System cannot be automatically initiated due to two or more inoperable, untripped Reactor Vessel Water Level—Low Low (Level 2) channels such that the trip system loses initiation capability. The 1 hour Completion Time from discovery of loss of initiation capability is acceptable because it minimizes risk while allowing time for restoration or tripping of channels.

Because of the redundancy of sensors available to provide initiation signals and the fact that the RCIC System is not assumed in any accident or transient analysis, an allowable out of service time of 24 hours has been shown to be acceptable (Ref. 1) to permit restoration of any inoperable channel to OPERABLE status. If the inoperable channel cannot be restored to OPERABLE status within the allowable out of service time, the channel must be placed in the tripped condition per Required Action B.2. Placing the inoperable channel in trip would conservatively compensate for the inoperability, restore capability to accommodate a single failure, and allow operation to continue. Alternately, if it is not desired to place the channel in trip (e.g., as in the case where placing the inoperable channel in trip would result in an initiation), Condition E must be entered and its Required Action taken.

(continued)

BASES

ACTIONS (continued)

C.1

A risk based analysis was performed and determined that an allowable out of service time of 24 hours (Ref. 1) is acceptable to permit restoration of any inoperable channel to OPERABLE status (Required Action C.1). A Required Action (similar to Required Action B.1) limiting the allowable out of service time, if a loss of automatic RCIC initiation capability exists, is not required. This Condition applies to the Reactor Vessel Water Level—High (Level 8) Function whose logic is arranged such that any inoperable channel will result in a loss of automatic RCIC initiation capability (closure of the RCIC steam supply valve). As stated above, this loss of automatic RCIC initiation capability was analyzed and determined to be acceptable. The Required Action does not allow placing a channel in trip since this action would not necessarily result in a safe state for the channel in all events.

D.1, D.2.1, and D.2.2

Required Action D.1 is intended to ensure that appropriate actions are taken if multiple, inoperable, untripped channels within the same Function result in automatic component initiation capability being lost for the feature(s). For Required Action D.1, the RCIC System is the only associated feature. In this case, automatic initiation capability is lost if two Function 3 channels are inoperable and untripped. In this situation (loss of automatic suction swap), the 24 hour allowance of Required Actions D.2.1 and D.2.2 is only appropriate after Action D.1 has been performed. Action D.1 requires that the RCIC System be declared inoperable within 1 hour from discovery of loss of RCIC initiation capability. As noted, Required Action D.1 is only applicable if the RCIC pump suction is not aligned to the suppression pool since, if aligned, the Function is already performed.

(continued)

BASES

ACTIONS

D.1, D.2.1, and D.2.2 (continued)

The Completion Time is intended to allow the operator time to evaluate and repair any discovered inoperabilities. This Completion Time also allows for an exception to the normal "time zero" for beginning the allowed outage time "clock." For Required Action D.1, the Completion Time only begins upon discovery that the RCIC System cannot be automatically aligned to the suppression pool due to two inoperable, untripped channels in the same Function. The 1 hour Completion Time from discovery of loss of initiation capability is acceptable because it minimizes risk while allowing time for restoration or tripping of channels.

Because the RCIC System is not assumed in any accident or transient analysis, an allowable out of service time of 24 hours has been shown to be acceptable (Ref. 1) to permit restoration of any inoperable channel to OPERABLE status. If the inoperable channel cannot be restored to OPERABLE status within the allowable out of service time, the channel must be placed in the tripped condition per Required Action D.2.1, which performs the intended function of the channel. Alternatively, Required Action D.2.2 allows the manual alignment of the RCIC suction to the suppression pool, which also performs the intended function. If Required Action D.2.1 or D.2.2 is performed, measures should be taken to ensure that the RCIC System piping remains filled with water. If it is not desired to perform Required Actions D.2.1 and D.2.2 (e.g., as in the case where shifting the suction source could drain down the RCIC suction piping), Condition E must be entered and its Required Action taken.

E.1

With any Required Action and associated Completion Time not met, the RCIC System may be incapable of performing the intended function, and the RCIC System must be declared inoperable immediately.

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS

As noted in the beginning of the SRs, the SRs for each RCIC System instrumentation Function are found in the SRs column of Table 3.3.5.2-1.

The Surveillances are modified by a Note to indicate that when a channel is placed in an inoperable status solely for performance of required Surveillances, entry into associated Conditions and Required Actions may be delayed as follows: (a) for up to 6 hours for Function 2 and (b) for up to 6 hours for Functions 1 and 3, provided the associated Function maintains trip capability. Upon completion of the Surveillance, or expiration of the 6 hour allowance, the channel must be returned to OPERABLE status or the applicable Condition entered and Required Actions taken. This Note is based on the reliability analysis (Ref. 1) assumption of the average time required to perform channel surveillance. That analysis demonstrated that the 6 hour testing allowance does not significantly reduce the probability that the RCIC will initiate when necessary.

SR 3.3.5.2.1

Performance of the CHANNEL CHECK once every 12 hours ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the parameter indicated on one channel to a parameter on other similar channels. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value. Significant deviations between the instrument channels could be an indication of excessive instrument drift in one of the channels or something even more serious. A CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

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

(continued)

BASES

SURVEILLANCE REQUIREMENTS

SR 3.3.5.2.1 (continued)

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

SR 3.3.5.2.2

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

The Frequency of 92 days is based on the reliability analysis of Reference 1.

SR 3.3.5.2.3

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

The Frequency of SR 3.3.5.2.3 is based upon the assumption of a 24 month calibration interval in the determination of the magnitude of equipment drift in the setpoint analysis.

SR 3.3.5.2.4

The LOGIC SYSTEM FUNCTIONAL TEST demonstrates the OPERABILITY of the required initiation logic for a specific channel. The system functional testing performed in LCO 3.5.3 overlaps this Surveillance to provide complete testing of the safety function.

(continued)

BASES

SURVEILLANCE REQUIREMENTS

SR 3.3.5.2.4 (continued)

While this Surveillance can be performed with the reactor at power for some of the Functions, operating experience has shown that these components will pass the Surveillance when performed at the 24 month Frequency. Therefore, the Frequency was found to be acceptable from a reliability standpoint.

REFERENCES

1. GENE-770-06-2, "Addendum to Bases for Changes to Surveillance Test Intervals and Allowed Out-of-Service Times for Selected Instrumentation Technical Specifications," February 1991.

B 3.3 INSTRUMENTATION

B 3.3.6.1 Primary Containment Isolation Instrumentation

BASES

BACKGROUND

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

The isolation instrumentation includes the sensors, relays, and switches that are necessary to cause initiation of primary containment and reactor coolant pressure boundary (RCPB) isolation. Most channels include electronic equipment (e.g., trip units) that compares measured input signals with pre-established setpoints. When the setpoint is exceeded, the channel output relay actuates, which then outputs a primary containment isolation signal to the isolation logic. Functional diversity is provided by monitoring a wide range of independent parameters. The input parameters to the isolation logics are (a) reactor vessel water level, (b) reactor pressure, (c) main steam line (MSL) flow measurement, (d) main steam line radiation, (e) main steam line pressure, (f) drywell pressure, (g) high pressure coolant injection (HPCI) and reactor core isolation cooling (RCIC) steam line flow, (h) HPCI and RCIC steam line pressure, (i) reactor water cleanup (RWCU) flow, (j) Standby Liquid Control (SLC) System initiation, (k) area ambient temperatures, (l) reactor building ventilation and refueling floor ventilation exhaust radiation, and (m) main stack radiation. Redundant sensor input signals from each parameter are provided for initiation of isolation.

Primary containment isolation instrumentation has inputs to the trip logic of the isolation functions listed below.

(continued)

BASES

BACKGROUND (continued)

1. Main Steam Line Isolation

Most MSL Isolation Functions receive inputs from four channels. The outputs from these channels are combined in a one-out-of-two taken twice logic to initiate isolation of the Group I isolation valves (MSIVs and MSL drains, MSL sample lines, and recirculation loop sample line valves). To initiate a Group I isolation, both trip systems must be tripped.

The exceptions to this arrangement are the Main Steam Line Flow—High Function and Main Steam Tunnel Temperature—High Functions. The Main Steam Line Flow—High Function uses 16 flow channels, four for each steam line. One channel from each steam line inputs to one of the four trip strings. Two trip strings make up each trip system and both trip systems must trip to cause an MSL isolation. Each trip string has four inputs (one per MSL), any one of which will trip the trip string. The trip systems are arranged in a one-out-of-two taken twice logic. This is effectively a one-out-of-eight taken twice logic arrangement to initiate a Group I isolation. The Main Steam Tunnel Temperature—High Function receives input from 16 channels. The logic is arranged similar to the Main Steam Line Flow—High Function except that high temperature on any channel is not related to a specific MSL.

2. Primary Containment Isolation

Most Primary Containment Isolation Functions receive inputs from four channels. The outputs from these channels are arranged in a one-out-of-two taken twice logic. Isolation of inboard and outboard primary containment isolation valves occurs when both trip systems are in trip.

The exception to this arrangement is the Main Stack Monitor Radiation—High Function. This Function has two channels, whose outputs are arranged in two trip systems which use a one-out-of-one logic. Each trip system isolates one valve per associated penetration. The Main Stack Monitor Radiation—High Function will isolate vent and purge valves greater than two inches in diameter during containment purging (Ref. 2).

The valves isolated by each of the Primary Containment Isolation Functions are listed in Reference 1.

(continued)

BASES

BACKGROUND (continued)

3., 4. High Pressure Coolant Injection System Isolation and Reactor Core Isolation Cooling System Isolation

The Steam Line Flow—High Functions that isolate HPCI and RCIC receive input from two channels, with each channel comprising one trip system using a one-out-of-one logic. Each of the two trip systems in each isolation group (HPCI and RCIC) is connected to the two valves on each associated penetration. Each HPCI and RCIC Steam Line Flow—High channel has a time delay relay to prevent isolation due to flow transients during startup.

The HPCI and RCIC Isolation Functions for Drywell Pressure—High and Steam Supply Line Pressure—Low receive inputs from four channels. The outputs from these channels are combined in a one-out-of-two taken twice logic to initiate isolation of the associated valves.

The HPCI and RCIC Compartment and Steam Line Area Temperature—High Functions receive input from 16 channels. The logic is similar to the Main Steam Tunnel Temperature—High Function.

The HPCI and RCIC Steam Line Flow—High Functions, Steam Supply Line Pressure—Low Functions, and Compartment and Steam Line Area Temperature—High Functions isolate the associated steam supply and turbine exhaust valves and pump suction valves. The HPCI and RCIC Drywell Pressure—High Functions isolate the HPCI and RCIC test return line valves. The HPCI and RCIC Drywell Pressure—High Functions, in conjunction with the Steam Supply Line Pressure—Low Functions, isolate the HPCI and RCIC turbine exhaust vacuum relief valves.

5. Reactor Water Cleanup System Isolation

The Reactor Vessel Water Level—Low (Level 3) Isolation Function receives input from four reactor vessel water level channels. The outputs from the reactor vessel water level channels are connected into a one-out-of-two taken twice logic which isolates both the inboard and outboard isolation valves. The RWCU Flow—High Function receives input from two channels, with each channel in one trip system using a one-out-of-one logic, with one channel tripping the inboard valve and one channel tripping the outboard valves. The SLC

(continued)

BASES

BACKGROUND

5. Reactor Water Cleanup System Isolation (continued)

System Isolation Function receives input from two channels with each channel in one trip system using a one-out-of-one logic. When either SLC pump is started remotely, one channel trips the inboard isolation valve and one channel isolates the outboard isolation valves.

The RWCU Isolation Function isolates the inboard and outboard RWCU pump suction penetration and the outboard valve at the RWCU connection to reactor feedwater.

6. Shutdown Cooling System Isolation

The Reactor Vessel Water Level—Low (Level 3) Function receives input from four reactor vessel water level channels. The outputs from the channels are connected to a one-out-of-two taken twice logic, which isolates both valves on the RHR shutdown cooling pump suction penetration. The Reactor Pressure—High Function receives input from two channels, with each channel in one trip system using a one-out-of-one logic. Each trip system is connected to both valves on the RHR shutdown cooling pump suction penetration.

7. Feedwater Recirculation Isolation

The Reactor Pressure—High Function receives inputs from four channels. The outputs from the four channels are connected into a one-out-of-two taken twice logic which isolates the feedwater recirculation valves.

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

The isolation signals generated by the primary containment isolation instrumentation are implicitly assumed in the safety analyses of References 1 and 3 to initiate closure of valves to limit offsite doses. Refer to LCO 3.6.1.3, "Primary Containment Isolation Valves (PCIVs)," Applicable Safety Analyses Bases for more detail of the safety analyses.

Primary containment isolation instrumentation satisfies Criterion 3 of the NRC Policy Statement. Certain instrumentation Functions are retained for other reasons and are described below in the individual Functions discussion.

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

The OPERABILITY of the primary containment instrumentation is dependent on the OPERABILITY of the individual instrumentation channel Functions specified in Table 3.3.6.1-1. Each Function must have a required number of OPERABLE channels, with their setpoints within the specified Allowable Values, where appropriate. A channel is inoperable if its actual trip setting is not within its required Allowable Value. The actual setpoint is calibrated consistent with applicable setpoint methodology assumptions.

Allowable Values, where applicable, are specified for each Primary Containment Isolation Function specified in the Table. Trip setpoints are specified in the setpoint calculations. The trip setpoints are selected to ensure that the setpoints do not exceed the Allowable Value between CHANNEL CALIBRATIONS. Operation with a trip setting less conservative than the trip setpoint, but within its Allowable Value, is acceptable. Trip setpoints are those predetermined values of output at which an action should take place. The setpoints are compared to the actual process parameter (e.g., reactor vessel water level), and when the measured output value of the process parameter exceeds the setpoint, the associated device (e.g., trip unit) changes state. The analytic or design limits are derived from the limiting values of the process parameters obtained from the safety analysis or other appropriate documents. The Allowable Values are derived from the analytic or design limits, corrected for calibration, process, and instrument errors. The trip setpoints are determined from analytical or design limits, corrected for calibration, process, and instrument errors, as well as, instrument drift. In selected cases, the Allowable Values and trip setpoints are determined by engineering judgement or historically accepted practice relative to the intended function of the channel. The trip setpoints determined in this manner provide adequate protection by assuring instrument and process uncertainties expected for the environments during the operating time of the associated channels are accounted for.

Certain Emergency Core Cooling Systems (ECCS) and RCIC valves (e.g., minimum flow) also serve the dual function of automatic PCIVs. The signals that isolate these valves are also associated with the automatic initiation of the ECCS

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

and RCIC. The instrumentation requirements and ACTIONS associated with these signals are addressed in LCO 3.3.5.1, "Emergency Core Cooling Systems (ECCS) Instrumentation," and LCO 3.3.5.2, "Reactor Core Isolation Cooling (RCIC) System Instrumentation," and are not included in this LCO.

In general, the individual Functions are required to be OPERABLE in MODES 1, 2, and 3 consistent with the Applicability for LCO 3.6.1.1, "Primary Containment." Functions that have different Applicabilities are discussed below in the individual Functions discussion.

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

Main Steam Line Isolation

1.a. Reactor Vessel Water Level—Low Low Low (Level 1)

Low reactor pressure vessel (RPV) water level indicates that the capability to cool the fuel may be threatened. Should RPV water level decrease too far, fuel damage could result. Therefore, isolation of the MSIVs and other interfaces with the reactor vessel occurs to prevent offsite dose limits from being exceeded. The Reactor Vessel Water Level—Low Low Low (Level 1) Function is one of the many Functions assumed to be OPERABLE and capable of providing isolation signals. The Reactor Vessel Water Level—Low Low Low (Level 1) Function associated with isolation is assumed in the analysis of the recirculation line break (Ref. 1). The isolation of the MSLs on Level 1 supports actions to ensure that offsite dose limits are not exceeded for a DBA.

Reactor vessel water level signals are initiated from four level transmitters that sense the difference between the pressure due to a constant column of water (reference leg) and the pressure due to the actual water level (variable leg) in the vessel. Four channels of Reactor Vessel Water Level—Low Low Low (Level 1) Function are available and are required to be OPERABLE to ensure that no single instrument failure can preclude the isolation function.

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

1.a. Reactor Vessel Water Level—Low Low Low (Level 1) (continued)

The Reactor Vessel Water Level—Low Low Low (Level 1) Allowable Value is chosen to be the same as the ECCS Level 1 Allowable Value (LCO 3.3.5.1) to ensure that the MSLs isolate on a potential loss of coolant accident (LOCA) to prevent offsite doses from exceeding 10 CFR 100 limits.

This Function isolates MSIVs, MSL drains, MSL sample lines and recirculation loop sample line valves.

1.b. Main Steam Line Pressure—Low

Low MSL pressure indicates that there may be a problem with the turbine pressure regulation, which could result in a low reactor vessel water level condition and the RPV cooling down more than 100°F/hr if the pressure loss is allowed to continue. The Main Steam Line Pressure—Low Function is directly assumed in the analysis of the pressure regulator failure (Ref. 3). For this event, the closure of the MSIVs ensures that the RPV temperature change limit (100°F/hr) is not reached. In addition, this Function supports actions to ensure that Safety Limit 2.1.1.1 is not exceeded. (This Function closes the MSIVs prior to pressure decreasing below 785 psig, which results in a scram due to MSIV closure, thus reducing reactor power to < 25% RTP.)

The MSL low pressure signals are initiated from four transmitters that are connected to the MSL header. The transmitters are arranged such that, even though physically separated from each other, each transmitter is able to detect low MSL pressure. Four channels of Main Steam Line Pressure—Low Function are available and are required to be OPERABLE to ensure that no single instrument failure can preclude the isolation function.

The Allowable Value was selected to be high enough to prevent excessive RPV depressurization.

The Main Steam Line Pressure—Low Function is only required to be OPERABLE in MODE 1 since this is when the assumed transient can occur (Ref. 1).

This Function isolates MSIVs, MSL drains, MSL sample lines and recirculation loop sample line valves.

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

1.c. Main Steam Line Flow—High

Main Steam Line Flow—High is provided to detect a break of the MSL and to initiate closure of the MSIVs. If the steam were allowed to continue flowing out of the break, the reactor would depressurize and the core could uncover. If the RPV water level decreases too far, fuel damage could occur. Therefore, the isolation is initiated on high flow to prevent or minimize core damage. The Main Steam Line Flow—High Function is directly assumed in the analysis of the main steam line break (MSLB) (Ref. 3). The isolation action, along with the scram function of the Reactor Protection System (RPS), ensures that the fuel peak cladding temperature remains below the limits of 10 CFR 50.46 and offsite doses do not exceed the 10 CFR 100 limits.

The MSL flow signals are initiated from 16 transmitters that are connected to the four MSLs. The transmitters are arranged such that, even though physically separated from each other, all four connected to one MSL would be able to detect the high flow. Four channels of Main Steam Line Flow—High Function for each MSL (two channels per trip system) are available and are required to be OPERABLE so that no single instrument failure will preclude detecting a break in any individual MSL.

The Allowable Value is chosen to ensure that offsite dose limits are not exceeded due to the break.

This Function isolates MSIVs, MSL drains, MSL sample lines and recirculation loop sample line valves.

1.d. Main Steam Line—High Radiation

The Main Steam Line—High Radiation Function is provided to detect gross release of fission products from the fuel and to initiate closure of the MSIVs. The trip setting is set low enough so that a high radiation trip results from a design basis rod drop accident and high enough above background radiation levels in the vicinity of the main steam lines so that spurious trips at rated power are avoided. The Main Steam Line—High Radiation Function is directly assumed in the analysis of the control rod drop accident (Ref. 3).

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

1.d. Main Steam Line—High Radiation (continued)

The Main Steam Line—High Radiation signals are initiated from four gamma sensitive instruments. Four channels are available and are required to be OPERABLE to ensure that no single instrument failure can preclude the isolation function.

The Allowable Value is chosen to ensure that offsite dose limits are not exceeded.

This Function isolates MSIVs, MSL drains, MSL sample lines and recirculation loop sample line valves.

1.e. Main Steam Tunnel Temperature—High

The Main Steam Tunnel Temperature Function is provided to detect a break in a main steam line and provides diversity to the high flow instrumentation.

Main Steam Tunnel Temperature signals are initiated from resistance temperature detectors (RTDs) located along the main steam line between the drywell wall and the turbine. Sixteen channels of Main Steam Tunnel Temperature—High Function are available and are required to be OPERABLE to ensure that no single instrument failure can preclude the isolation function.

The Allowable Value is chosen to detect a leak equivalent to between 1% and 10% rated steam flow.

This Function isolates MSIVs, MSL drains, MSL sample lines and recirculation loop sample line valves.

Primary Containment Isolation

2.a. Reactor Vessel Water Level—Low (Level 3)

Low RPV water level indicates that the capability to cool the fuel may be threatened. The valves whose penetrations communicate with the primary containment are isolated to limit the release of fission products. The isolation of the primary containment on Level 3 supports actions to ensure that offsite dose limits of 10 CFR 100 are not exceeded.

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

2.a. Reactor Vessel Water Level—Low (Level 3) (continued)

The Reactor Vessel Water Level—Low (Level 3) Function associated with isolation is implicitly assumed in the UFSAR analysis as these leakage paths are assumed to be isolated post LOCA.

Reactor Vessel Water Level—Low (Level 3) signals are initiated from level transmitters that sense the difference between the pressure due to a constant column of water (reference leg) and the pressure due to the actual water level (variable leg) in the vessel. Four channels of Reactor Vessel Water Level—Low (Level 3) Function are available and are required to be OPERABLE to ensure that no single instrument failure can preclude the isolation function.

The Reactor Vessel Water Level—Low (Level 3) Allowable Value was chosen to be the same as the RPS Level 3 scram Allowable Value (LCO 3.3.1.1), since isolation of these valves is not critical to orderly plant shutdown.

This Function isolates the Group II(A) valves listed in Reference 1 with the exception of RWCU isolation valves and RHR shutdown cooling pump suction valves which are addressed in Functions 5.c and 6.b, respectively.

2.b. Drywell Pressure—High

High drywell pressure can indicate a break in the RCPB inside the primary containment. The isolation of some of the primary containment isolation valves on high drywell pressure supports actions to ensure that offsite dose limits of 10 CFR 100 are not exceeded. The Drywell Pressure—High Function, associated with isolation of the primary containment, is implicitly assumed in the UFSAR accident analysis as these leakage paths are assumed to be isolated post LOCA.

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

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

2.b. Drywell Pressure–High (continued)

The Allowable Value was selected to be the same as the ECCS Drywell Pressure–High Allowable Value (LCO 3.3.5.1), since this may be indicative of a LOCA inside primary containment.

This Function isolates the Group II(B) valves listed in Reference 1.

2.c. Main Stack Monitor Radiation–High

Main stack monitor radiation is an indication that the release of radioactive material may exceed established limits. Therefore, when Main Stack Monitor Radiation–High is detected when there is flow through the Standby Gas Treatment System, an isolation of primary containment purge supply and exhaust penetrations is initiated to limit the release of fission products. However, this Function is not assumed in any accident or transient analysis in the UFSAR because other leakage paths (e.g., MSIVs) are more limiting.

The drywell radiation signals are initiated from radiation detectors that isokinetically sample the main stack utilizing sample pumps. Two channels of Main Stack Radiation–High Function are available and are required to be OPERABLE to ensure that no single instrument failure can preclude the isolation function.

The Allowable Value is set below the maximum allowable release limit in accordance with the Offsite Dose Calculation Manual (ODCM).

This Function isolates the containment vent and purge valves and other Group III(E) valves listed in Reference 1.

2.d., 2.e. Reactor Building Ventilation and Refueling Floor Ventilation Exhaust Radiation–High

High secondary containment exhaust radiation is an indication of possible gross failure of the fuel cladding. The release may have originated from the primary containment due to a break in the RCPB. When Reactor Building or Refueling Floor Ventilation Exhaust Radiation–High is detected, the affected ventilation pathway and primary

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

2.d., 2.e. Reactor Building Ventilation and Refueling Floor Ventilation Exhaust Radiation—High (continued)

containment purge supply and exhaust valves are isolated to limit the release of fission products. Additionally, Ventilation Exhaust Radiation—High Function initiates Standby Gas Treatment System.

The Ventilation Exhaust Radiation—High signals are initiated from radiation detectors that are located on the ventilation exhaust piping coming from the reactor building and the refueling floor zones, respectively. The signal from each detector is input to an individual monitor whose trip outputs are assigned to an isolation channel. Four channels of Reactor Building Ventilation Exhaust—High Function and four channels of Refueling Floor Ventilation Exhaust—High Function are available and are required to be OPERABLE to ensure that no single instrument failure can preclude the isolation function.

The Allowable Values are chosen to promptly detect gross failure of the fuel cladding during a refueling accident.

These Functions isolate the Group III(C) and III(D) valves listed in Reference 1.

High Pressure Coolant Injection and Reactor Core Isolation Cooling Systems Isolation

3.a., 3.b., 4.a., 4.b. HPCI and RCIC Steam Line Flow—High and Time Delay Relays

Steam Line Flow—High Functions are provided to detect a break of the RCIC or HPCI steam lines and initiate closure of the steam line isolation valves of the appropriate system. If the steam is allowed to continue flowing out of the break, the reactor will depressurize and the core can uncover. Therefore, the isolations are initiated on high flow to prevent or minimize core damage. The isolation action, along with the scram function of the RPS, ensures that the fuel peak cladding temperature remains below the limits of 10 CFR 50.46. Specific credit for these Functions is not assumed in any UFSAR accident analyses since the

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

3.a., 3.b., 4.a., 4.b. HPCI and RCIC Steam Line Flow-High and Time Delay Relays (continued)

bounding analysis is performed for large breaks such as recirculation and MSL breaks. However, these instruments prevent the RCIC or HPCI steam line breaks from becoming bounding.

The HPCI and RCIC Steam Line Flow—High signals are initiated from transmitters (two for HPCI and two for RCIC) that are connected to the system steam lines. A time delay is provided to prevent isolation due to high flow transients during startup with one Time Delay Relay channel associated with each Steam Line Flow—High channel. Two channels of both HPCI and RCIC Steam Line Flow—High Functions and the associated Time Delay Relays are available and are required to be OPERABLE to ensure that no single instrument failure can preclude the isolation function.

The Allowable Values for Steam Line Flow—High Function and associated Time Delay Relay Function are chosen to be low enough to ensure that the trip occurs to maintain the MSLB event as the bounding event.

These Functions isolate the associated HPCI and RCIC steam supply and turbine exhaust valves and pump suction valves.

3.c., 4.c. HPCI and RCIC Steam Supply Line Pressure—Low

Low MSL pressure indicates that the pressure of the steam in the HPCI or RCIC turbine may be too low to continue operation of the associated system's turbine. These isolations prevent radioactive gases and steam from escaping through the pump shaft seals into the reactor building but are primarily for equipment protection and are also assumed for long term containment isolation. However, they also provide a diverse signal to indicate a possible system break. These instruments are included in Technical Specifications (TS) because of the potential for risk due to possible failure of the instruments preventing HPCI and RCIC initiations (Ref. 4).

The HPCI and RCIC Steam Supply Line Pressure—Low signals are initiated from transmitters (four for HPCI and four for RCIC) that are connected to the system steam line. Four

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

3.c., 4.c. HPCI and RCIC Steam Supply Line Pressure—Low (continued)

channels of both HPCI and RCIC Steam Supply Line Pressure—Low Functions are available and are required to be OPERABLE to ensure that no single instrument failure can preclude the isolation function.

The Allowable Values are selected to be high enough to prevent damage to the system's turbine.

These Functions isolate the associated HPCI and RCIC steam supply and turbine exhaust valves and pump suction valves.

3.d., 4.d. Drywell Pressure—High (Vacuum Breakers)

High drywell pressure can indicate a break in the RCPB. The HPCI and RCIC isolation of the turbine exhaust vacuum breakers is provided to prevent communication with the drywell when high drywell pressure exists. The HPCI and RCIC turbine exhaust vacuum breaker isolation occurs following a permissive from the associated Steam Supply Line Pressure—Low Function which indicates that the system is no longer required or capable of performing coolant injection. The isolation of the HPCI and RCIC turbine exhaust vacuum breakers by Drywell Pressure—High is indirectly assumed in the UFSAR accident analysis because the turbine exhaust leakage path is not assumed to contribute to offsite doses.

High drywell pressure signals are initiated from pressure transmitters that sense the pressure in the drywell. Four channels for both HPCI and RCIC Drywell Pressure—High (Vacuum Breakers) Functions are available and are required to be OPERABLE to ensure that no single instrument failure can preclude the isolation function.

The Allowable Value was selected to be the same as the ECCS Drywell Pressure—High Allowable Value (LCO 3.3.5.1), since this is indicative of a LOCA inside primary containment.

This Function isolates the associated HPCI and RCIC vacuum relief valves and test return line valves.

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

3.e., 4.e. HPCI and RCIC Compartment and Steam Line Area Temperature-High

HPCI and RCIC Compartment and Steam Line Area temperatures are provided to detect a leak from the associated system steam piping. The isolation occurs when a very small leak has occurred and is diverse to the high flow instrumentation. If the small leak is allowed to continue without isolation, offsite dose limits may be reached.

These Functions are not assumed in any UFSAR transient or accident analysis, since bounding analyses are performed for large breaks such as recirculation or MSL breaks.

HPCI and RCIC Compartment and Steam Line Area Temperature-High signals are initiated from resistance temperature detectors (RTDs) that are appropriately located to protect the system that is being monitored. The HPCI and RCIC Compartment and Steam Line Area Temperature-High Functions each use 16 temperature channels. Sixteen channels for each HPCI and RCIC Compartment and Steam Line Area Temperature-High Function are available and are required to be OPERABLE to ensure that no single instrument failure can preclude the isolation function.

The Allowable Values are set low enough to detect a leak.

These Functions isolate the associated HPCI and RCIC steam supply and turbine exhaust valves and pump suction valves.

Reactor Water Cleanup (RWCU) System Isolation

5.a. RWCU Flow-High

The high flow signal is provided to detect a break in the RWCU System. Should the reactor coolant continue to flow out of the break, offsite dose limits may be exceeded. Therefore, isolation of the RWCU System is initiated when high RWCU flow is sensed to prevent exceeding offsite doses. This Function is not assumed in any UFSAR transient or accident analysis, since bounding analyses are performed for large breaks such as MSLBs.

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

5.a. RWCU Flow—High (continued)

The high RWCU flow signals are initiated from transmitters that are connected to the pump suction line of the RWCU System. Two channels of RWCU Flow—High Function are available and are required to be OPERABLE to ensure that no single instrument failure can preclude the isolation function.

The RWCU Flow—High Allowable Value ensures that a break of the RWCU piping is detected.

This Function isolates the inboard and outboard RWCU pump suction penetration and the outboard valve at the RWCU connection to reactor feedwater.

5.b. Standby Liquid Control (SLC) System Initiation

The isolation of the RWCU System is required when the SLC System has been initiated to prevent dilution and removal of the boron solution by the RWCU System (Ref. 5). SLC System initiation signals are initiated from the remote SLC System start switch.

There is no Allowable Value associated with this Function since the channels are mechanically actuated based solely on the position of the SLC System initiation switch.

Two channels of the SLC System Initiation Function are available and are required to be OPERABLE only in MODES 1 and 2, since these are the only MODES where the reactor can be critical, and these MODES are consistent with the Applicability for the SLC System (LCO 3.1.7).

This Function isolates the inboard and outboard RWCU pump suction penetration and the outboard valve at the RWCU connection to reactor feedwater.

5.c. Reactor Vessel Water Level—Low (Level 3)

Low RPV water level indicates that the capability to cool the fuel may be threatened. Should RPV water level decrease too far, fuel damage could result. Therefore, isolation of some interfaces with the reactor vessel occurs to isolate the potential sources of a break. The isolation of the RWCU System on Level 3 supports actions to ensure that the fuel

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

5.c. Reactor Vessel Water Level—Low (Level 3) (continued)

peak cladding temperature remains below the limits of 10 CFR 50.46. The Reactor Vessel Water Level—Low (Level 3) Function associated with RWCU isolation is not directly assumed in the UFSAR safety analyses because the RWCU System line break is bounded by breaks of larger systems (recirculation and MSL breaks are more limiting).

Reactor Vessel Water Level—Low (Level 3) signals are initiated from four level transmitters that sense the difference between the pressure due to a constant column of water (reference leg) and the pressure due to the actual water level (variable leg) in the vessel. Four channels of Reactor Vessel Water Level—Low (Level 3) Function are available and are required to be OPERABLE to ensure that no single instrument failure can preclude the isolation function.

The Reactor Vessel Water Level—Low (Level 3) Allowable Value was chosen to be the same as the RPS Reactor Vessel Water Level—Low (Level 3) Allowable Value (LCO 3.3.1.1), since the capability to cool the fuel may be threatened.

This Function isolates the inboard and outboard RWCU suction penetration and the outboard valve at the RWCU connection to reactor feedwater.

Shutdown Cooling System Isolation

6.a. Reactor Pressure—High

The Reactor Pressure—High Function is provided to isolate the shutdown cooling portion of the Residual Heat Removal (RHR) System. This Function is provided only for equipment protection to prevent an intersystem LOCA scenario, and credit for the Function is not assumed in the accident or transient analysis in the UFSAR.

The Reactor Pressure—High signals are initiated from two switches that are connected to different taps on the RPV. Two channels of Reactor Pressure—High Function are available and are required to be OPERABLE to ensure that no single instrument failure can preclude the isolation function. The Function is only required to be OPERABLE in

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

6.a. Reactor Pressure—High (continued)

MODES 1, 2, and 3, since these are the only MODES in which the reactor can be pressurized; thus, equipment protection is needed. The Allowable Value was chosen to be low enough to protect the system equipment from overpressurization.

This Function isolates both RHR shutdown cooling pump suction valves.

6.b. Reactor Vessel Water Level—Low (Level 3)

Low RPV water level indicates that the capability to cool the fuel may be threatened. Should RPV water level decrease too far, fuel damage could result. Therefore, isolation of some reactor vessel interfaces occurs to begin isolating the potential sources of a break. The Reactor Vessel Water Level—Low (Level 3) Function associated with RHR Shutdown Cooling System isolation is not directly assumed in safety analyses because a break of the RHR Shutdown Cooling System is bounded by breaks of the recirculation and MSL. The RHR Shutdown Cooling System isolation on Level 3 supports actions to ensure that the RPV water level does not drop below the top of the active fuel during a vessel draindown event caused by a leak (e.g., pipe break or inadvertent valve opening) in the RHR Shutdown Cooling System.

Reactor Vessel Water Level—Low (Level 3) signals are initiated from four level transmitters that sense the difference between the pressure due to a constant column of water (reference leg) and the pressure due to the actual water level (variable leg) in the vessel. Four channels (two channels per trip system) of the Reactor Vessel Water Level—Low (Level 3) Function are available and are required to be OPERABLE to ensure that no single instrument failure can preclude the isolation function. As noted (footnote (a) to Table 3.3.6.1-1), only one channel per trip system (with an isolation signal available to one shutdown cooling pump suction isolation valve) of the Reactor Vessel Water Level—Low (Level 3) Function are required to be OPERABLE in MODES 4 and 5, provided the RHR Shutdown Cooling System integrity is maintained. System integrity is maintained provided the piping is intact and no maintenance is being performed that has the potential for draining the reactor vessel through the system.

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

6.b. Reactor Vessel Water Level—Low (Level 3) (continued)

The Reactor Vessel Water Level—Low (Level 3) Allowable Value was chosen to be the same as the RPS Reactor Vessel Water Level—Low (Level 3) Allowable Value (LCO 3.3.1.1), since the capability to cool the fuel may be threatened.

The Reactor Vessel Water Level—Low (Level 3) Function is only required to be OPERABLE in MODES 3, 4, and 5 to prevent this potential flow path from lowering the reactor vessel level to the top of the fuel. In MODES 1 and 2, another isolation (i.e., Reactor Pressure—High) and administrative controls ensure that this flow path remains isolated to prevent unexpected loss of inventory via this flow path.

This Function isolates both RHR shutdown cooling pump suction valves.

Feedwater Recirculation Isolation

7.a. Reactor Pressure—High

The Reactor Pressure—High Function is provided to isolate the feedwater recirculation line. This interlock is provided only for equipment protection to prevent an intersystem LOCA scenario, and credit for the interlock is not assumed in the accident or transient analysis in the UFSAR.

The Reactor Pressure—High signals are initiated from four transmitters that are connected to different taps on the RPV. Four channels of Reactor Pressure—High Function are available and are required to be OPERABLE to ensure that no single instrument failure can preclude the isolation function. The Function is only required to be OPERABLE in MODES 1, 2, and 3, since these are the only MODES in which the reactor can be pressurized; thus, equipment protection is needed. The Allowable Value was chosen to be low enough to protect the system equipment from overpressurization.

This Function isolates the feedwater recirculation valves.

(continued)

BASES (continued)

ACTIONS

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

A.1

Because of the diversity of sensors available to provide isolation signals and the redundancy of the isolation design, an allowable out of service time of 12 hours for Functions 1.d, 2.a, and 2.b and 24 hours for Functions other than Functions 1.d, 2.a, and 2.b has been shown to be acceptable (Refs. 6 and 7) to permit restoration of any inoperable channel to OPERABLE status. This out of service time is only acceptable provided the associated Function is still maintaining isolation capability (refer to Required Action B.1 Bases). If the inoperable channel cannot be restored to OPERABLE status within the allowable out of service time, the channel must be placed in the tripped condition per Required Action A.1. Placing the inoperable channel in trip would conservatively compensate for the inoperability, restore capability to accommodate a single failure, and allow operation to continue with no further restrictions. Alternately, if it is not desired to place the channel in trip (e.g., as in the case where placing the inoperable channel in trip would result in an isolation), Condition C must be entered and its Required Action taken.

(continued)

BASES

ACTIONS (continued)

B.1

Required Action B.1 is intended to ensure that appropriate actions are taken if multiple, inoperable, untripped channels within the same Function result in redundant isolation capability being lost for the associated penetration flow path(s). For those MSL, Primary Containment, HPCI, RCIC, RWCU, SDC, and Feedwater Recirculation Isolation Functions, where actuation of both trip systems is needed to isolate a penetration, the Functions are considered to be maintaining isolation capability when sufficient channels are OPERABLE or in trip (or the associated trip system in trip), such that both trip systems will generate a trip signal from the given Function on a valid signal. For those Primary Containment, HPCI, RCIC, RWCU, and SDC isolation functions, where actuation of one trip system is needed to isolate a penetration, the Functions are considered to be maintaining isolation capability when sufficient channels are OPERABLE or in trip, such that one trip system will generate a trip signal from the given function on a valid signal. This ensures that at least one of the PCIVs in the associated penetration flow path can receive an isolation signal from the given Function. For all Functions except 1.c, 1.e, 2.c, 3.a, 3.b, 3.e, 4.a, 4.b, 4.e, 5.a, 5.b, and 6.a, this would require both trip systems to have one channel OPERABLE or in trip. For Function 1.c, this would require both trip systems to have one channel, associated with each MSL, OPERABLE or in trip. For Functions 1.e, 3.e and 4.e, each Function consists of channels that monitor several locations within a given area (e.g., different locations within the main steam tunnel area). Therefore, this would require both trip systems to have one channel per location OPERABLE or in trip. For Functions 2.c, 3.a, 3.b, 4.a, 4.b, 5.a, and 6.a, this would require one trip system to have one channel OPERABLE or in trip.

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

(continued)

BASES

ACTIONS

B.1 (continued)

Entry into Condition B and Required Action B.1 may be necessary to avoid an MSL isolation transient when recovering from a temporary loss of ventilation in the main steam line tunnel area. As allowed by LCO 3.0.2 (and discussed in the Bases of LCO 3.0.2), the plant may intentionally enter this Condition to avoid an MSL isolation transient during the restoration of ventilation flow, and then raise the setpoints for the Main Steam Tunnel Temperature—High Function to 250°F causing all channels of Main Steam Tunnel Temperature—High Function to be inoperable. However, during the period that multiple Main Steam Tunnel Temperature—High Function channels are inoperable due to this intentional action, an additional compensatory measure is deemed necessary and shall be taken: an operator shall observe control room indications of the duct temperature so the main steam line isolation valves may be promptly closed in the event of a rapid increase in MSL tunnel temperature indicative of a steam line break.

C.1

Required Action C.1 directs entry into the appropriate Condition referenced in Table 3.3.6.1-1. The applicable Condition specified in Table 3.3.6.1-1 is Function and MODE or other specified condition dependent and may change as the Required Action of a previous Condition is completed. Each time an inoperable channel has not met any Required Action of Condition A or B and the associated Completion Time has expired, Condition C will be entered for that channel and provides for transfer to the appropriate subsequent Condition.

D.1, D.2.1, and D.2.2

If the channel is not restored to OPERABLE status or placed in trip within the allowed Completion Time, the plant must be placed in a MODE or other specified condition in which the LCO does not apply. This is done by placing the plant in at least MODE 3 within 12 hours and in MODE 4 within 36 hours (Required Actions D.2.1 and D.2.2). Alternately, the associated MSLs may be isolated (Required Action D.1),

(continued)

BASES

ACTIONS

D.1, D.2.1, and D.2.2 (continued)

and, if allowed (i.e., plant safety analysis allows operation with an MSL isolated), operation with that MSL isolated may continue. Isolating the affected MSL accomplishes the safety function of the inoperable channel. 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.

E.1

If the channel is not restored to OPERABLE status or placed in trip within the allowed Completion Time, the plant must be placed in a MODE or other specified condition in which the LCO does not apply. This is done by placing the plant in at least MODE 2 within 6 hours.

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

F.1

If the channel is not restored to OPERABLE status or placed in trip within the allowed Completion Time, plant operations may continue if the affected penetration flow path(s) is isolated. Isolating the affected penetration flow path(s) accomplishes the safety function of the inoperable channels. Alternately, if it is not desired to isolate the affected penetration flow path(s) (e.g., as in the case where isolating the penetration flow path(s) could result in a reactor scram), Condition G must be entered and its Required Actions taken. The 1 hour Completion Time is acceptable because it minimizes risk while allowing sufficient time for plant operations personnel to isolate the affected penetration flow path(s).

(continued)

BASES

ACTIONS (continued)

G.1 and G.2

If the channel is not restored to OPERABLE status or placed in trip within the allowed Completion Time, or the Required Action of Condition F is not met and the associated Completion Time has expired, the plant must be placed in a MODE or other specified condition in which the LCO does not apply. This is done by placing the plant in at least MODE 3 within 12 hours and in MODE 4 within 36 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

H.1 and H.2

If the channel is not restored to OPERABLE status or placed in trip within the allowed Completion Time, the associated SLC subsystem(s) is declared inoperable or the RWCU System is isolated. Since this Function is required to ensure that the SLC System performs its intended function, sufficient remedial measures are provided by declaring the associated SLC subsystems inoperable or isolating the RWCU System.

The 1 hour Completion Time is acceptable because it minimizes risk while allowing sufficient time for personnel to isolate the RWCU System.

I.1 and I.2

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

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS

As noted at the beginning of the SRs, the SRs for each Primary Containment Isolation instrumentation Function are found in the SRs column of Table 3.3.6.1-1.

The Surveillances are modified by a Note to indicate that when a channel is placed in an inoperable status solely for performance of required Surveillances, entry into associated Conditions and Required Actions may be delayed for up to 6 hours provided the associated Function maintains trip capability. Upon completion of the Surveillance, or expiration of the 6 hour allowance, the channel must be returned to OPERABLE status or the applicable Condition entered and Required Actions taken. This Note is based on the reliability analysis (Refs. 6 and 7) assumption of the average time required to perform channel surveillance. That analysis demonstrated that the 6 hour testing allowance does not significantly reduce the probability that the PCIVs will isolate the penetration flow path(s) when necessary.

SR 3.3.6.1.1

Performance of the CHANNEL CHECK once every 12 hours ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the parameter indicated on one channel to a similar parameter on other channels. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value. Significant deviations between the instrument channels could be an indication of excessive instrument drift in one of the channels or of something even more serious. A CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

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

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

(continued)

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.6.1.2

A CHANNEL FUNCTIONAL TEST is performed on each required channel to ensure that the entire channel will perform the intended function. Any setpoint adjustment shall be consistent with the assumptions of the current plant specific setpoint methodology. For Function 1.e, 3.e, and 4.e channels, verification that trip settings are less than or equal to the specified Allowable Value during the CHANNEL FUNCTIONAL TEST is not required since the installed indication instrumentation does not provide accurate indication of the trip setting. This is considered acceptable since the magnitude of drift assumed in the setpoint calculation is based on a 24 month calibration interval.

The 92 day Frequency of SR 3.3.6.1.2 is based on the reliability analysis described in Reference 7.

SR 3.3.6.1.3, SR 3.3.6.1.4, SR 3.3.6.1.5, and SR 3.3.6.1.6

A CHANNEL CALIBRATION is a complete check of the instrument loop and the sensor. This test verifies the channel responds to the measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drifts between successive calibrations, consistent with the assumptions of the current setpoint methodology. SR 3.3.6.1.6, however, is only a calibration of the radiation detectors using a standard radiation source.

As noted for SR 3.3.6.1.3, the main steam line radiation detectors (Function 1.d) are excluded from CHANNEL CALIBRATION due to ALARA reasons (when the plant is operating, the radiation detectors are generally in a high radiation area; the steam tunnel). This exclusion is acceptable because the radiation detectors are passive devices, with minimal drift. The radiation detectors are calibrated in accordance with SR 3.3.6.1.6 on a 24 month Frequency.

(continued)

BASES

SURVEILLANCE REQUIREMENTS

SR 3.3.6.1.3, SR 3.3.6.1.4, SR 3.3.6.1.5, and SR 3.3.6.1.6 (continued)

The 92 day Frequency of SR 3.3.6.1.3 is conservative with respect to the magnitude of equipment drift assumed in the setpoint analysis. The Frequency of SR 3.3.6.1.4 is based on the assumption of an 18 month calibration interval in the determination of the magnitude of equipment drift in the setpoint analysis. The Frequencies of SR 3.3.6.1.5 and SR 3.3.6.1.6 are based on the assumption of a 24 month calibration interval in the determination of the magnitude of equipment drift in the setpoint analysis.

SR 3.3.6.1.7

The LOGIC SYSTEM FUNCTIONAL TEST demonstrates the OPERABILITY of the required isolation logic for a specific channel. The system functional testing performed on PCIVs in LCO 3.6.1.3 overlaps this Surveillance to provide complete testing of the assumed safety function.

While this Surveillance can be performed with the reactor at power for some of the Functions, operating experience has shown these components will pass the Surveillance when performed at the 24 month Frequency. Therefore, the Frequency was found to be acceptable from a reliability standpoint.

REFERENCES

1. UFSAR, Section 7.3.

2. NRC Safety Evaluation Report for Amendment Numbers 156 and 158 to Facility Operating License Numbers DPR-44 and DPR-56, Peach Bottom Atomic Power Station, Unit Nos. 2 and 3, September 7, 1990.

3. UFSAR, Chapter 14.

4. NEDO-31466, "Technical Specification Screening Criteria Application and Risk Assessment," November 1987.

5. UFSAR, Section 4.9.3.

(continued)

BASES

6. NEDC-31677P-A, "Technical Specification Improvement Analysis for BWR Isolation Actuation Instrumentation," July 1990.

7. NEDC-30851P-A Supplement 2, "Technical Specifications Improvement Analysis for BWR Isolation Instrumentation Common to RPS and ECCS Instrumentation," March 1989.

B 3.3 INSTRUMENTATION

B 3.3.6.2 Secondary Containment Isolation Instrumentation

BASES

BACKGROUND

The secondary containment isolation instrumentation automatically initiates closure of appropriate secondary containment isolation valves (SCIVs) and starts the Standby Gas Treatment (SGT) System. The function of these systems, in combination with other accident mitigation systems, is to limit fission product release during and following postulated Design Basis Accidents (DBAs) (Ref. 1). Secondary containment isolation and establishment of vacuum with the SGT System within the required time limits ensures that fission products that leak from primary containment following a DBA, or are released outside primary containment, or are released during certain operations when primary containment is not required to be OPERABLE are maintained within applicable limits.

The isolation instrumentation includes the sensors, relays, and switches that are necessary to cause initiation of secondary containment isolation. Most channels include electronic equipment (e.g., trip units) that compares measured input signals with pre-established setpoints. When the setpoint is exceeded, the channel output relay actuates, which then outputs a secondary containment isolation signal to the isolation logic. Functional diversity is provided by monitoring a wide range of independent parameters. The input parameters to the isolation logic are (1) reactor vessel water level, (2) drywell pressure, (3) reactor building ventilation exhaust high radiation, and (4) refueling floor ventilation exhaust high radiation. Redundant sensor input signals from each parameter are provided for initiation of isolation.

The outputs of the channels are arranged in a one-out-of-two taken twice logic. Automatic isolation valves (dampers) isolate and SGT subsystems start when both trip systems are in trip. Operation of both trip systems is required to isolate the secondary containment and provide for the necessary filtration of fission products.

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

The isolation signals generated by the secondary containment isolation instrumentation are implicitly assumed in the safety analyses of References 1 and 2 to initiate closure of valves and start the SGT System to limit offsite doses.

Refer to LCO 3.6.4.2, "Secondary Containment Isolation Valves (SCIVs)," and LCO 3.6.4.3, "Standby Gas Treatment (SGT) System," Applicable Safety Analyses Bases for more detail of the safety analyses.

The secondary containment isolation instrumentation satisfies Criterion 3 of the NRC Policy Statement. Certain instrumentation Functions are retained for other reasons and are described below in the individual Functions discussion.

The OPERABILITY of the secondary containment isolation instrumentation is dependent on the OPERABILITY of the individual instrumentation channel Functions. Each Function must have the required number of OPERABLE channels with their setpoints set within the specified Allowable Values, as shown in Table 3.3.6.2-1. The actual setpoint is calibrated consistent with applicable setpoint methodology assumptions. A channel is inoperable if its actual trip setting is not within its required Allowable Value.

Allowable Values are specified for each Function specified in the Table. Trip setpoints are specified in the setpoint calculations. The trip setpoints are selected to ensure that the setpoints do not exceed the Allowable Value between CHANNEL CALIBRATIONS. Operation with a trip setting less conservative than the trip setpoint, but within its Allowable Value, is acceptable.

Trip setpoints are those predetermined values of output at which an action should take place. The setpoints are compared to the actual process parameter (e.g., reactor vessel water level), and when the measured output value of the process parameter exceeds the setpoint, the associated device (e.g., trip unit) changes state. The analytic or design limits are derived from the limiting values of the process parameters obtained from the safety analysis or other appropriate documents. The Allowable Values are derived from the analytic or design limits, corrected for calibration, process, and instrument errors. The trip setpoints are then determined from analytical or design limits, corrected for calibration, process, and instrument

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

errors, as well as, instrument drift. In selected cases, the Allowable Values and trip setpoints are determined by engineering judgement or historically accepted practice relative to the intended function of the channel. The trip setpoints determined in this manner provide adequate protection by assuring instrument and process uncertainties expected for the environments during the operating time of the associated channels are accounted for.

In general, the individual Functions are required to be OPERABLE in the MODES or other specified conditions when SCIVs and the SGT System are required.

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

1. Reactor Vessel Water Level – Low (Level 3)

Low reactor pressure vessel (RPV) water level indicates that the capability to cool the fuel may be threatened. Should RPV water level decrease too far, fuel damage could result. An isolation of the secondary containment and actuation of the SGT System are initiated in order to minimize the potential of an offsite dose release. The Reactor Vessel Water Level – Low (Level 3) Function is one of the Functions assumed to be OPERABLE and capable of providing isolation and initiation signals. The isolation and initiation systems on Reactor Vessel Water Level – Low (Level 3) support actions to ensure that any offsite releases are within the limits calculated in the safety analysis.

Reactor Vessel Water Level – Low (Level 3) signals are initiated from level transmitters that sense the difference between the pressure due to a constant column of water (reference leg) and the pressure due to the actual water level (variable leg) in the vessel. Four channels of Reactor Vessel Water Level – Low (Level 3) Function are available and are required to be OPERABLE in MODES 1, 2, and 3 to ensure that no single instrument failure can preclude the isolation function.

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

1. Reactor Vessel Water Level – Low (Level 3) (continued)

The Reactor Vessel Water Level – Low (Level 3) Allowable Value was chosen to be the same as the RPS Level 3 scram Allowable Value (LCO 3.3.1.1), since isolation of these valves and SGT System start are not critical to orderly plant shutdown.

The Reactor Vessel Water Level – Low (Level 3) Function is required to be OPERABLE in MODES 1, 2, and 3 where considerable energy exists in the Reactor Coolant System (RCS); thus, there is a probability of pipe breaks resulting in significant releases of radioactive steam and gas. In MODES 4 and 5, the probability and consequences of these events are low due to the RCS pressure and temperature limitations of these MODES; thus, this Function is not required. In addition, the Function is also required to be OPERABLE during operations with a potential for draining the reactor vessel (OPDRVs) because the capability of isolating potential sources of leakage must be provided to ensure that offsite dose limits are not exceeded if core damage occurs.

2. Drywell Pressure – High

High drywell pressure can indicate a break in the reactor coolant pressure boundary (RCPB). An isolation of the secondary containment and actuation of the SGT System are initiated in order to minimize the potential of an offsite dose release. The isolation on high drywell pressure supports actions to ensure that any offsite releases are within the limits calculated in the safety analysis. The Drywell Pressure – High Function associated with isolation is not assumed in any UFSAR accident or transient analyses but will provide an isolation and initiation signal. It is retained for the overall redundancy and diversity of the secondary containment isolation instrumentation as required by the NRC approved licensing basis.

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

2. Drywell Pressure–High (continued)

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

The Allowable Value was chosen to be the same as the ECCS Drywell Pressure–High Function Allowable Value (LCO 3.3.5.1) since this is indicative of a loss of coolant accident (LOCA).

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

3., 4. Reactor Building Ventilation and Refueling Floor Ventilation Exhaust Radiation–High

High secondary containment exhaust radiation is an indication of possible gross failure of the fuel cladding. The release may have originated from the primary containment due to a break in the RCPB or during refueling due to a fuel handling accident. When Ventilation Exhaust Radiation–High is detected, secondary containment isolation and actuation of the SGT System are initiated to limit the release of fission products as assumed in the UFSAR safety analyses (Ref. 4).

The Ventilation Exhaust Radiation–High signals are initiated from radiation detectors that are located on the ventilation exhaust piping coming from the reactor building and the refueling floor zones, respectively. The signal from each detector is input to an individual monitor whose trip outputs are assigned to an isolation channel. Four

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

3. 4. Reactor Building Ventilation and Refueling Floor Ventilation Exhaust Radiation—High (continued)

channels of Reactor Building Ventilation Exhaust Radiation—High Function and four channels of Refueling Floor Ventilation Exhaust Radiation—High Function are available and are required to be OPERABLE to ensure that no single instrument failure can preclude the isolation function.

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

The Reactor Building Ventilation and Refueling Floor Ventilation Exhaust Radiation—High Functions are required to be OPERABLE in MODES 1, 2, and 3 where considerable energy exists; thus, there is a probability of pipe breaks resulting in significant releases of radioactive steam and gas. In MODES 4 and 5, the probability and consequences of these events are low due to the RCS pressure and temperature limitations of these MODES; thus, these Functions are not required. In addition, the Functions are also required to be OPERABLE during CORE ALTERATIONS, OPDRVs, and movement of irradiated fuel assemblies in the secondary containment, because the capability of detecting radiation releases due to fuel failures (due to fuel uncovery or dropped fuel assemblies) must be provided to ensure that offsite dose limits are not exceeded.

ACTIONS

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

(continued)

BASES

ACTIONS (continued)

A.1

Because of the diversity of sensors available to provide isolation signals and the redundancy of the isolation design, an allowable out of service time of 12 hours for Functions 1 and 2, and 24 hours for Functions other than Functions 1 and 2, has been shown to be acceptable (Refs. 5 and 6) to permit restoration of any inoperable channel to OPERABLE status. This out of service time is only acceptable provided the associated Function is still maintaining isolation capability (refer to Required Action B.1 Bases). If the inoperable channel cannot be restored to OPERABLE status within the allowable out of service time, the channel must be placed in the tripped condition per Required Action A.1. Placing the inoperable channel in trip would conservatively compensate for the inoperability, restore capability to accommodate a single failure, and allow operation to continue. Alternately, if it is not desired to place the channel in trip (e.g., as in the case where placing the inoperable channel in trip would result in an isolation), Condition C must be entered and its Required Actions taken.

B.1

Required Action B.1 is intended to ensure that appropriate actions are taken if multiple, inoperable, untripped channels within the same Function result in a complete loss of isolation capability for the associated penetration flow path(s) or a complete loss of automatic initiation capability for the SGT System. A Function is considered to be maintaining secondary containment isolation capability when sufficient channels are OPERABLE or in trip, such that both trip systems will generate a trip signal from the given Function on a valid signal. This ensures that at least one of the two SCIVs in the associated penetration flow path and at least one SGT subsystem can be initiated on an isolation signal from the given Function. For Functions 1, 2, 3, and 4, this would require both trip systems to have one channel OPERABLE or in trip.

(continued)

BASES

ACTIONS

B.1 (continued)

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

C.1.1, C.1.2, C.2.1, and C.2.2

If any Required Action and associated Completion Time of Condition A or B are not met, the ability to isolate the secondary containment and start the SGT System cannot be ensured. Therefore, further actions must be performed to ensure the ability to maintain the secondary containment function. Isolating the associated secondary containment penetration flow path(s) and starting the associated SGT subsystem (Required Actions C.1.1 and C.2.1) performs the intended function of the instrumentation and allows operation to continue.

Alternately, declaring the associated SCIVs or SGT subsystem(s) inoperable (Required Actions C.1.2 and C.2.2) is also acceptable since the Required Actions of the respective LCOs (LCO 3.6.4.2 and LCO 3.6.4.3) provide appropriate actions for the inoperable components.

One hour is sufficient for plant operations personnel to establish required plant conditions or to declare the associated components inoperable without unnecessarily challenging plant systems.

SURVEILLANCE REQUIREMENTS

As noted at the beginning of the SRs, the SRs for each Secondary Containment Isolation instrumentation Function are located in the SRs column of Table 3.3.6.2-1.

(continued)

BASES

SURVEILLANCE REQUIREMENTS (continued)

The Surveillances are modified by a Note to indicate that when a channel is placed in an inoperable status solely for performance of required Surveillances, entry into associated Conditions and Required Actions may be delayed for up to 6 hours provided the associated Function maintains secondary containment isolation capability. Upon completion of the Surveillance, or expiration of the 6 hour allowance, the channel must be returned to OPERABLE status or the applicable Condition entered and Required Actions taken. This Note is based on the reliability analysis (Refs. 5 and 6) assumption that of the average time required to perform channel surveillance. That analysis demonstrated the 6 hour testing allowance does not significantly reduce the probability that the SCIVs will isolate the associated penetration flow paths and that the SGT System will initiate when necessary.

SR 3.3.6.2.1

Performance of the CHANNEL CHECK once every 12 hours ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the parameter indicated on one channel to a similar parameter on other channels. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value. Significant deviations between the instrument channels could be an indication of excessive instrument drift in one of the channels or something even more serious. A CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

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

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

(continued)

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.6.2.2

A CHANNEL FUNCTIONAL TEST is performed on each required channel to ensure that the entire channel will perform the intended function. Any setpoint adjustment shall be consistent with the assumptions of the current plant specific setpoint methodology. The Frequency of 92 days for SR 3.3.6.2.2 is based on the reliability analysis of References 5 and 6.

SR 3.3.6.2.3 and SR 3.3.6.2.4T

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

The Frequencies of SR 3.3.6.2.3 and SR 3.3.6.2.4 are based on the assumption of the magnitude of equipment drift in the setpoint analysis.

SR 3.3.6.2.5

The LOGIC SYSTEM FUNCTIONAL TEST demonstrates the OPERABILITY of the required isolation logic for a specific channel. The system functional testing performed on SCIVs and the SGT System in LCO 3.6.4.2 and LCO 3.6.4.3, respectively, overlaps this Surveillance to provide complete testing of the assumed safety function.

While this Surveillance can be performed with the reactor at power for some of the Functions, operating experience has shown that these components will pass the Surveillance when performed at the 24 month Frequency. Therefore, the Frequency was found to be acceptable from a reliability standpoint.

(continued)

BASES (continued)

REFERENCES

1. UFSAR, Section 14.6.

2. UFSAR, Chapter 14.

3. UFSAR, Section 14.6.5.

4. UFSAR, Sections 14.6.3 and 14.6.4.

5. NEDC-31677P-A, "Technical Specification Improvement Analysis for BWR Isolation Actuation Instrumentation," July 1990.

6. NEDC-30851P-A Supplement 2, "Technical Specifications Improvement Analysis for BWR Isolation Instrumentation Common to RPS and ECCS Instrumentation," March 1989.

B 3.3 INSTRUMENTATION

B 3.3.7.1 Main Control Room Emergency Ventilation (MCREV) System Instrumentation

BASES

BACKGROUND

The MCREV System is designed to provide a radiologically controlled environment to ensure the habitability of the control room for the safety of control room operators under all plant conditions. Two independent MCREV subsystems are each capable of fulfilling the stated safety function. The instrumentation and controls for the MCREV System automatically initiate action to pressurize the main control room (MCR) to minimize the consequences of radioactive material in the control room environment.

In the event of a Control Room Air Intake Radiation—High signal, the MCREV System is automatically started in the pressurization mode. The outside air from the normal ventilation intake is then passed through one of the charcoal filter subsystems. Sufficient outside air is drawn in through the normal ventilation intake to maintain the MCR slightly pressurized with respect to the turbine building.

The MCREV System instrumentation has two trip systems with two Control Room Air Intake Radiation—High channels in each trip system. The outputs of the Control Room Air Intake Radiation—High channels are arranged in two trip systems, which use a one-out-of-two logic. The tripping of both trip systems will initiate both MCREV subsystems. The channels include electronic equipment (e.g., trip units) that compares measured input signals with pre-established setpoints. When the setpoint is exceeded, the channel output relay actuates, which then outputs a MCREV System initiation signal to the initiation logic.

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

The ability of the MCREV System to maintain the habitability of the MCR is explicitly assumed for certain accidents as discussed in the UFSAR safety analyses (Refs. 1, 2, and 3). MCREV System operation ensures that the radiation exposure of control room personnel, through the duration of any one of the postulated accidents, does not exceed acceptable limits.

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

MCREV System instrumentation satisfies Criterion 3 of the NRC Policy Statement.

The OPERABILITY of the MCREV System instrumentation is dependent upon the OPERABILITY of the Control Room Air Intake Radiation—High instrumentation channel Function. The Function must have a required number of OPERABLE channels, with their setpoints within the specified Allowable Values, where appropriate. A channel is inoperable if its actual trip setting is not within its required Allowable Value. The actual setpoint is calibrated consistent with applicable setpoint methodology assumptions.

Allowable Values are specified for the MCREV System Control Room Air Intake Radiation—High Function. Trip setpoints are specified in the setpoint calculations. The trip setpoints are selected to ensure that the setpoints do not exceed the Allowable Value between successive CHANNEL CALIBRATIONS. Operation with a trip setting less conservative than the trip setpoint, but within its Allowable Value, is acceptable. Trip setpoints are those predetermined values of output at which an action should take place. The setpoints are compared to the actual process parameter (e.g., control room air intake radiation), and when the measured output value of the process parameter exceeds the setpoint, the associated device changes state. The analytic limits are derived from the limiting values of the process parameters obtained from the safety analysis. The Allowable Values are derived from the analytic limits, corrected for calibration, process, and instrument errors. The trip setpoints are determined from analytical or design limits, corrected for calibration, process, and instrument errors, as well as, instrument drift. The trip setpoints derived in this manner provide adequate protection by ensuring instrument and process uncertainties expected for the environments during the operating time of the associated channels are accounted for.

The control room air intake radiation monitors measure radiation levels in the fresh air supply plenum. A high radiation level may pose a threat to MCR personnel; thus, automatically initiating the MCREV System.

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

The Control Room Air Intake Radiation–High Function consists of four independent monitors. Two channels of Control Room Air Intake Radiation–High per trip system are available and are required to be OPERABLE to ensure that no single instrument failure can preclude MCREV System initiation. The Allowable Value was selected to ensure protection of the control room personnel.

The Control Room Air Intake Radiation–High Function is required to be OPERABLE in MODES 1, 2, and 3 and during CORE ALTERATIONS, OPDRVs, and movement of irradiated fuel assemblies in the secondary containment, to ensure that control room personnel are protected during a LOCA, fuel handling event, or vessel draindown event. During MODES 4 and 5, when these specified conditions are not in progress (e.g., CORE ALTERATIONS), the probability of a LOCA or fuel damage is low; thus, the Function is not required.

ACTIONS

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

A.1 and A.2

Because of the redundancy of sensors available to provide initiation signals and the redundancy of the MCREV System design, an allowable out of service time of 6 hours has been shown to be acceptable (Ref. 4), to permit restoration of any inoperable channel to OPERABLE status. However, this out of service time is only acceptable provided the Control Room Air Intake Radiation–High Function is still maintaining MCREV System initiation capability. The Function is considered to be maintaining MCREV System

(continued)

BASES

ACTIONS

A.1 and A.2 (continued)

initiation capability when sufficient channels are OPERABLE or in trip such that the two trip systems will generate an initiation signal from the given Function on a valid signal. For the Control Room Air Intake Radiation—High Function, this would require the two trip systems to have one channel per trip system OPERABLE or in trip. In this situation (loss of MCREV System initiation capability), the 6 hour allowance of Required Action A.2 is not appropriate. If the Function is not maintaining MCREV System initiation capability, the MCREV System must be declared inoperable within 1 hour of discovery of the loss of MCREV System initiation capability in both trip systems.

The 1 hour Completion Time (A.1) is acceptable because it minimizes risk while allowing time for restoring or tripping of channels.

If the inoperable channel cannot be restored to OPERABLE status within the allowable out of service time, the channel must be placed in the tripped condition per Required Action A.2. Placing the inoperable channel in trip would conservatively compensate for the inoperability, restore capability to accommodate a single failure, and allow operation to continue. Alternately, if it is not desired to place the channel in trip (e.g., as in the case where placing the inoperable channel in trip would result in an initiation), Condition B must be entered and its Required Action taken.

B.1 and B.2

With any Required Action and associated Completion Time not met, the associated MCREV subsystem(s) must be placed in operation per Required Action B.1 to ensure that control room personnel will be protected in the event of a Design Basis Accident. The method used to place the MCREV subsystem(s) in operation must provide for automatically re-initiating the subsystem(s) upon restoration of power following a loss of power to the MCREV subsystem(s). Alternately, if it is not desired to start the subsystem(s), the MCREV subsystem(s) associated with inoperable, untripped

(continued)

BASES

ACTIONS

B.1 and B.2 (continued)

channels must be declared inoperable within 1 hour. Since each trip system can affect both MCREV subsystems, Required Actions B.1 and B.2 can be performed independently on each MCREV subsystem. That is, one MCREV subsystem can be placed in operation (Required Action B.1) while the other MCREV subsystem can be declared inoperable (Required Action B.2).

The 1 hour Completion Time is intended to allow the operator time to place the MCREV subsystem(s) in operation. The 1 hour Completion Time is acceptable because it minimizes risk while allowing time for placing the associated MCREV subsystem(s) in operation, or for entering the applicable Conditions and Required Actions for the inoperable MCREV subsystem(s).

SURVEILLANCE REQUIREMENTS

The Surveillances are modified by a Note to indicate that when a channel is placed in an inoperable status solely for performance of required Surveillances, entry into associated Conditions and Required Actions may be delayed for up to 6 hours, provided the associated Function maintains MCREV System initiation capability. Upon completion of the Surveillance, or expiration of the 6 hour allowance, the channel must be returned to OPERABLE status or the applicable Condition entered and Required Actions taken. This Note is based on the reliability analysis (Ref. 4) assumption of the average time required to perform channel surveillance. That analysis demonstrated that the 6 hour testing allowance does not significantly reduce the probability that the MCREV System will initiate when necessary.

SR 3.3.7.1.1

Performance of the CHANNEL CHECK once every 12 hours ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the parameter indicated on one channel to a similar parameter on other channels. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value. Significant deviations between the instrument channels could be an indication of excessive instrument drift in one of the channels or something even more serious. A CHANNEL CHECK will detect

(continued)

BASES

SURVEILLANCE REQUIREMENTS

SR 3.3.7.1.1 (continued)

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

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

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

SR 3.3.7.1.2

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

The Frequency of 92 days is based on the reliability analyses of Reference 4.

SR 3.3.7.1.3

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

The Frequency is based upon the assumption of an 18 month calibration interval in the determination of the magnitude of the equipment drift in the setpoint analysis.

(continued)

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.7.1.4

The LOGIC SYSTEM FUNCTIONAL TEST demonstrates the OPERABILITY of the required initiation logic for a specific channel. The system functional testing performed in LCO 3.7.4, "Main Control Room Emergency Ventilation (MCREV) System," overlaps this Surveillance to provide complete testing of the assumed safety function.

While this Surveillance can be performed with the reactor at power, operating experience has shown these components will pass the Surveillance when performed at the 24 month Frequency. Therefore, the Frequency was found to be acceptable from a reliability standpoint.

REFERENCES

1. UFSAR, Section 10.13.

2. UFSAR, Section 12.3.4.

3. UFSAR, Section 14.9.1.5.

4. GENE-770-06-1, "Bases for Changes to Surveillance Test Intervals and Allowed Out-of-Service Times for Selected Instrumentation Technical Specifications," February 1991.

B 3.3 INSTRUMENTATION

B 3.3.8.1 Loss of Power (LOP) Instrumentation

BASES

BACKGROUND

Successful operation of the required safety functions of the Emergency Core Cooling Systems (ECCS) is dependent upon the availability of adequate power for energizing various components such as pump motors, motor operated valves, and the associated control components. The LOP instrumentation monitors the 4 kV emergency buses voltage. Offsite power is the preferred source of power for the 4 kV emergency buses. If the LOP instrumentation detects that voltage levels are too low, the buses are disconnected from the offsite power sources and connected to the onsite diesel generator (DG) power sources.

Each Unit 2 4 kV emergency bus has its own independent LOP instrumentation and associated trip logic. The voltage for each bus is monitored at five levels, which can be considered as two different undervoltage Functions: one level of loss of voltage and four levels of degraded voltage. The Functions cause various bus transfers and disconnects. The degraded voltage Function is monitored by four undervoltage relays per source and the loss of voltage Function is monitored by one undervoltage relay for each emergency bus. The degraded voltage outputs and the loss of voltage outputs are arranged in a one-out-of-one trip logic configuration. Each channel consists of four protective relays that compare offsite source voltages with pre-established setpoints. When the sensed voltage is below the setpoint for a degraded voltage channel, the preferred offsite source breaker to the 4 kV emergency bus is tripped and autotransfer to the alternate offsite source is initiated. If the alternate source does not provide adequate voltage to the bus as sensed by its degraded grid relays, a diesel generator start signal is initiated.

A description of the Unit 3 LOP instrumentation is provided in the Bases for Unit 3 LCO 3.3.8.1.

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

The LOP instrumentation is required for Engineered Safety Features to function in any accident with a loss of offsite power. The required channels of LOP instrumentation ensure that the ECCS and other assumed systems powered from the DGs, provide plant protection in the event of any of the Reference 1 (UFSAR) analyzed accidents in which a loss of offsite power is assumed. The first level is loss of voltage. This loss of voltage level detects and disconnects the Class 1E buses from the offsite power source upon a total loss of voltage. The second level of undervoltage protection is provided by the four levels of degraded grid voltage relays which are set to detect a sustained low voltage condition. These degraded grid relays disconnect the Class 1E buses from the offsite power source if the degraded voltage condition exists for a time interval which could prevent the Class 1E equipment from achieving its safety function. The degraded grid relays also prevent the Class 1E equipment from sustaining damage from prolonged operation at reduced voltage. The combination of the loss of voltage relaying and the degraded grid relaying provides protection to the Class 1E distribution system for all credible conditions of voltage collapse or sustained voltage degradation. The initiation of the DGs on loss of offsite power, and subsequent initiation of the ECCS, ensure that the fuel peak cladding temperature remains below the limits of 10 CFR 50.46.

Accident analyses credit the loading of the DG based on the loss of offsite power during a loss of coolant accident. The diesel starting and loading times have been included in the delay time associated with each safety system component requiring DG supplied power following a loss of offsite power.

The LOP instrumentation satisfies Criterion 3 of the NRC Policy Statement.

The OPERABILITY of the LOP instrumentation is dependent upon the OPERABILITY of the individual instrumentation relay channel Functions specified in Table 3.3.8.1-1. Each Function must have a required number of OPERABLE channels per 4 kV emergency bus, with their setpoints within the specified Allowable Values except the bus undervoltage relay which does not have an Allowable Value. A degraded voltage channel is inoperable if its actual trip setpoint is not within its required Allowable Value. Setpoints are calibrated consistent with the Improved Instrument Setpoint Control Program (IISCP) methodology assumptions. (Note: Table 3.3.8.1-1 contains a note that prior to the implementation of modification 96-01511, the relay voltage and timer trip setpoint Allowable Vaulues for the indicated

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

functions remain at the previously approved values on a relay by relay basis.) The loss of voltage channel is inoperable if it will not start the diesel on a loss of power to a 4 kV emergency bus.

The Allowable Values are specified for each applicable Function in the Table 3.3.8.1-1. The nominal setpoints are selected to ensure that the setpoints do not exceed the Allowable Value between CHANNEL CALIBRATIONS. Operation with a trip setpoint within the Allowable Value, is acceptable. Trip setpoints are those predetermined values of output at which an action should take place. The setpoints are compared to the actual process parameter (e.g., voltage), and when the measured output value of the process parameter exceeds the setpoint, the protective relay output changes state. The Allowable Values were set equal to the limiting values determined by the voltage regulation calculation. The setpoints were corrected using IISCP methodology to account for relay drift, relay accuracy, potential transformer accuracy, measuring and test equipment accuracy margin, and includes a calibration leave alone zone. IISCP methodology utilizes the square root of the sum of the squares to combine random non-directional accuracy values. IISCP then includes relay drift, calibration leave alone zones, and margins. (Note: Table 3.3.8.1-1 contains a note that prior to the implementation of modification 96-01511, the relay voltage and timer trip setpoint Allowable Values for the indicated functions remain at the previously approved values on a relay by relay basis.) The setpoint assumes a nominal 35/1 potential transformer ratio.

The specific Applicable Safety Analyses, LCO, and Applicability discussions for Unit 2 LOP instrumentation are listed below on a Function by Function basis.

In addition, since some equipment required by Unit 2 is powered from Unit 3 sources, the Unit 3 LOP instrumentation supporting the required sources must also be OPERABLE. The OPERABILITY requirements for the Unit 3 LOP instrumentation is the same as described in this section, except Function 4 (4 kV Emergency Bus Undervoltage, Degraded Voltage LOCA) is not required to be OPERABLE, since this Function is related to a LOCA on Unit 3 only. The Unit 3 instrumentation is listed in Unit 3 Table 3.3.8.1-1.

1. 4 kV Emergency Bus Undervoltage (Loss of Voltage)

When both offsite sources are lost, a loss of voltage condition on a 4 kV emergency bus indicates that the respective emergency bus is unable to supply sufficient power for proper operation of the applicable equipment. Therefore, the power supply to the bus is transferred from offsite power to DG power. This ensures that adequate power will be available to the required equipment.

(continued)

BASES

APPLICABLE SAFETY ANALYSIS, LCO, and APPLICABILITY

1. 4 kV Emergency Bus Undervoltage (Loss of Voltage) (continued)

The single channel of 4 kV Emergency Bus Undervoltage (Loss of Voltage) Function per associated emergency bus is only required to be OPERABLE when the associated DG and offsite circuit are required to be OPERABLE. This ensures no single instrument failure can preclude the start of three of four DGs. (One channel inputs to each of the four DGs.) Refer to LCO 3.8.1, "AC Sources—Operating," and 3.8.2, "AC Sources—Shutdown," for Applicability Bases for the DGs.

2., 3., 4., 5. 4 kV Emergency Bus Undervoltage (Degraded Voltage)

A degraded voltage condition on a 4 kV emergency bus indicates that, while offsite power may not be completely lost to the respective emergency bus, available power may be insufficient for starting large ECCS motors without risking damage to the motors that could disable the ECCS function.

Therefore, power to the bus is transferred from offsite power to onsite DG power when there is insufficient offsite power to the bus. This transfer will occur only if the voltage of the preferred and alternate power sources drop below the Degraded Voltage Function Allowable Values (degraded voltage with a time delay) and the source breakers trip which causes the bus undervoltage relay to initiate the DG. This ensures that adequate power will be available to the required equipment.

Four Functions are provided to monitor degraded voltage at four different levels. These Functions are the Degraded Voltage Non-LOCA, Degraded Voltage LOCA, Degraded Voltage High Setting, and Degraded Voltage Low Setting. These relays monitor the following voltage levels with the following time delays: the Function 2 relay, 2286 - 2706 volts in approximately 2 seconds when source voltage is reduced abruptly to zero volts (inverse time delay); the Function 3 relay, 3409 - 3829 volts in approximately 30 seconds when source voltage is reduced abruptly to 2940 volts (inverse time delay); the Function 4 relay, 3766 - 3836 volts in approximately 10 seconds; and the Function 5 relay, 4116 - 4186 volts in approximately 60 seconds. (Note: Table 3.3.8.1-1 contains a note that prior to the implementation of modification 96-01511, the relay voltage and timer trip setpoint Allowable Values for the indicated functions remain at the previously approved values on a relay by relay basis.) The Function 2 and 3 relays are inverse time delay relays. These relays operate along a repeatable characteristic curve. With relay operation being inverse with time, for

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY

2., 3., 4., 5. 4 kV Emergency Bus Undervoltage (Degraded Voltage) (continued)

an abrupt reduction in voltage the relay operating time will be short; conversely, for a slight reduction in voltage, the operating time delay will be long.

The Degraded Voltage LOCA Function preserves the assumptions of the LOCA analysis and the combined Functions of the other relays preserves the assumptions of the accident sequence analysis in the UFSAR. The Degraded Voltage Non-LOCA Function provides assurance that equipment powered from the 4kV emergency buses is not damaged by degraded voltage that might occur under other than LOCA conditions. This degraded grid non-LOCA relay has an associated 60 second timer. This timer allows for offsite source transformer load tap changer operation. Degraded voltage conditions can be mitigated by tap changer operations and other manual actions. The 60 second timer provides the time for these actions to take place.

The degraded grid voltage Allowable Values are low enough to prevent inadvertent power supply transfer, but high enough to ensure that sufficient power is available to the required equipment. The Time Delay Allowable Values are long enough to provide time for the offsite power supply to recover to normal voltages, but short enough to ensure that sufficient power is available to the required equipment.

Two channels (one channel per source) of 4 kV Emergency Bus Degraded Voltage (Functions 2, 3, 4, and 5) per associated bus are required to be OPERABLE when the associated DG and offsite circuit are required to be OPERABLE. This ensures no single instrument failure can preclude the start of three of four DGs (each logic inputs to each of the four DGs). Refer to LCO 3.8.1 and LCO 3.8.2 for Applicability Bases for the DGs.

ACTIONS

A Note has been provided (Note 1) to modify the ACTIONS related to LOP instrumentation channels. Section 1.3, Completion Times, specifies that once a Condition has been entered, subsequent divisions, subsystems, components, or variables expressed in the Condition, discovered to be inoperable or not within limits, will not result in separate entry into the Condition. Section 1.3 also specifies that Required Actions of the Condition continue to apply for each additional failure, with Completion Times based on initial

(continued)

BASES

ACTIONS (continued)

entry into the Condition. However, the Required Actions for inoperable LOP instrumentation channels provide appropriate compensatory measures for separate inoperable channels. As such, a Note has been provided that allows separate Condition entry for each inoperable LOP instrumentation channel.

A.1

Pursuant to LCO 3.0.6, the AC Sources—Operating ACTIONS would not have to be entered even if the LOP instrumentation inoperability resulted in an inoperable offsite circuit. Therefore, the Required Action of Condition A is modified by a Note to indicate that when performance of a Required Action results in the inoperability of an offsite circuit, Actions for LCO 3.8.1, "AC Sources—Operating," must be immediately entered. A Unit 2 offsite circuit is considered to be inoperable if it is not supplying or not capable of supplying (due to loss of autotransfer capability) at least three Unit 2 4 kV emergency buses when the other offsite circuit is providing power or capable of supplying power to all four Unit 2 4 kV emergency buses. A Unit 2 offsite circuit is also considered to be inoperable if the Unit 2 4 kV emergency buses being powered or capable of being powered from the two offsite circuits are all the same when at least one of the two circuits does not provide power or is not capable of supplying power to all four Unit 2 4 kV emergency buses. Inoperability of a Unit 3 offsite circuit is the same as described for a Unit 2 offsite circuit, except that the circuit path is to the Unit 3 4 kV emergency buses required to be OPERABLE by LCO 3.8.7, "Distribution Systems—Operating." The Note allows Condition A to provide requirements for the loss of a LOP instrumentation channel without regard to whether an offsite circuit is rendered inoperable. LCO 3.8.1 provides appropriate restriction for an inoperable offsite circuit.

Required Action A.1 is applicable when one 4 kV emergency bus has one or two required Function 3 (Degraded Voltage High Setting) channels inoperable or when one 4 kV emergency bus has one or two required Function 5 (Degraded Voltage Non-LOCA) channels inoperable. In this Condition, the affected Function may not be capable of performing its intended function automatically for these buses. However, the operators would still receive indication in the control room of a degraded voltage condition on the unaffected buses and a manual transfer of the affected bus power supply to

(continued)

BASES

ACTIONS

A.1 (continued)

the alternate source could be made without damaging plant equipment. Therefore, Required Action A.1 allows 14 days to restore the inoperable channel(s) to OPERABLE status or place the inoperable channel(s) in trip. Placing the inoperable channel in trip would conservatively compensate for the inoperability, restore design trip capability to the LOP instrumentation, and allow operation to continue. Alternatively, if it is not desired to place the channel in trip (e.g., as in the case where placing the channel in trip would result in DG initiation), Condition D must be entered and its Required Action taken.

The 14 day Completion Time is intended to allow time to restore the channel(s) to OPERABLE status. The Completion Time takes into consideration the diversity of the Degraded Voltage Functions, the capabilities of the remaining OPERABLE LOP Instrumentation Functions on the affected 4 kV emergency bus and on the other 4 kV emergency buses (only one 4 kV emergency bus is affected by the inoperable channels), the fact that the Degraded Voltage High Setting and Degraded Voltage Non-LOCA Functions provide only a marginal increase in the protection provided by the voltage monitoring scheme, the low probability of the grid operating in the voltage band protected by these Functions, and the ability of the operators to perform the Functions manually.

B.1

Pursuant to LCO 3.0.6, the AC Sources—Operating ACTIONS would not have to be entered even if the LOP instrumentation inoperability resulted in an inoperable offsite circuit. Therefore, the Required Action of Condition B is modified by a Note to indicate that when performance of a Required Action results in the inoperability of an offsite circuit, Actions for LCO 3.8.1, "AC Sources—Operating," must be immediately entered. A Unit 2 offsite circuit is considered to be inoperable if it is not supplying or not capable of supplying (due to loss of autotransfer capability) at least three Unit 2 4 kV emergency buses when the other offsite circuit is providing power or capable of supplying power to all four Unit 2 4 kV emergency buses. A Unit 2 offsite circuit is also considered to be inoperable if the Unit 2 4 kV emergency buses being powered or capable of being powered from the two offsite circuits are all the same when at least one of the two circuits does not provide power or

(continued)

BASES

ACTIONS

B.1 (continued)

is not capable of supplying power to all four Unit 2 4 kV emergency buses. Inoperability of a Unit 3 offsite circuit is the same as described for a Unit 2 offsite circuit, except that the circuit path is to the Unit 3 4 kV emergency buses required to be OPERABLE by LCO 3.8.7, "Distribution Systems - Operating." This allows Condition B to provide requirements for the loss of a LOP instrumentation channel without regard to whether an offsite circuit is rendered inoperable. LCO 3.8.1 provides appropriate restriction for an inoperable offsite circuit.

Required Action B.1 is applicable when two 4 kV emergency buses have one required Function 3 (Degraded Voltage High Setting) channel inoperable, or when two 4 kV emergency buses have one required Function 5 (Degraded Voltage Non-LOCA) channel inoperable, or when one 4 kV emergency bus has one required Function 3 channel inoperable and a different 4 kV emergency bus has one required Function 5 channel inoperable. In this Condition, the affected Function may not be capable of performing its intended function automatically for these buses. However, the operators would still receive indication in the control room of a degraded voltage condition on the unaffected buses and a manual transfer of the affected bus power supply to the alternate source could be made without damaging plant equipment. Therefore, Required Action B.1 allows 24 hours to restore the inoperable channels to OPERABLE status or place the inoperable channels in trip. Placing the inoperable channel in trip would conservatively compensate for the inoperability, restore design trip capability to the LOP instrumentation, and allow operation to continue. Alternatively, if it is not desired to place the channel in trip (e.g., as in the case where placing the channel in trip would result in DG initiation), Condition D must be entered and its Required Action taken.

The 24 hour Completion Time is intended to allow time to restore the channel(s) to OPERABLE status. The Completion Time takes into consideration the diversity of the Degraded Voltage Functions, the capabilities of the remaining OPERABLE LOP Instrumentation Functions on the affected 4 kV emergency buses and on the other 4 kV emergency buses (only two 4 kV emergency buses are affected by the inoperable channels), the fact that the Degraded Voltage High Setting and Degraded Voltage Non-LOCA Functions provide only a

(continued)

BASES

ACTIONS

B.1 (continued)

marginal increase in the protection provided by the voltage monitoring scheme, the low probability of the grid operating in the voltage band protected by these Functions, and the ability of the operators to perform the Functions manually.

C.1

Pursuant to LCO 3.0.6, the AC Sources—Operating ACTIONS would not have to be entered even if the LOP Instrumentation inoperability resulted in an inoperable offsite circuit. Therefore, the Required Action of Condition C is modified by a Note to indicate that when performance of the Required Action results in the inoperability of an offsite circuit, Actions for LCO 3.8.1, "AC Sources—Operating," must be immediately entered. A Unit 2 offsite circuit is considered to be inoperable if it is not supplying or not capable of supplying (due to loss of autotransfer capability) at least three Unit 2 4 kV emergency buses when the other offsite circuit is providing power or capable of supplying power to all four Unit 2 4 kV emergency buses. A Unit 2 offsite circuit is also considered to be inoperable if the Unit 2 4 kV emergency buses being powered or capable of being powered from the two offsite circuits are all the same when at least one of the two circuits does not provide power or is not capable of supplying power to all four Unit 2 4 kV emergency buses. Inoperability of a Unit 3 offsite circuit is the same as described for a Unit 2 offsite circuit, except that the circuit path is to the Unit 3 4 kV emergency buses required to be OPERABLE by LCO 3.8.7, "Distribution Systems - Operating." The Note allows Condition C to provide requirements for the loss of a LOP instrumentation channel without regard to whether an offsite circuit is rendered inoperable. LCO 3.8.1 provides appropriate restriction for an inoperable offsite circuit.

Required Action C.1 is applicable when one or more 4 kV emergency buses have one or more required Function 1, 2, or 4 (the Loss of Voltage, the Degraded Voltage Low Setting, and the Degraded Voltage LOCA Functions, respectively) channels inoperable, or when one 4 kV emergency bus has one required Function 3 (Degraded Voltage High Setting) channel and one required Function 5 (Degraded Voltage Non-LOCA) channel inoperable, or when any combination of three or more required Function 3 and Function 5 channels are inoperable. In this Condition, the affected Function may not be capable

(continued)

BASES

ACTIONS

C.1 (continued)

of performing the intended function and the potential consequences associated with the inoperable channel(s) are greater than those resulting from Condition A or Condition B. Therefore, only 1 hour is allowed to restore the inoperable channel to OPERABLE status. If the inoperable channel cannot be restored to OPERABLE status within the allowable out of service time, the channel must be placed in the tripped condition per Required Action C.1. Placing the inoperable channel in trip would conservatively compensate for the inoperability, restore design trip capability to the LOP instrumentation, and allow operation to continue. Alternately, if it is not desired to place the channel in trip (e.g., as in the case where placing the channel in trip would result in a DG initiation), Condition D must be entered and its Required Action taken.

The Completion Time is based on the potential consequences associated with the inoperable channel(s) and is intended to allow the operator time to evaluate and repair any discovered inoperabilities. The 1 hour Completion Time is acceptable because it minimizes risk while allowing time for restoration or tripping of channels.

D.1

If any Required Action and associated Completion Time are not met, the associated Function is not capable of performing the intended function. Therefore, the associated DG(s) is declared inoperable immediately. This requires entry into applicable Conditions and Required Actions of LCO 3.8.1 and LCO 3.8.2, which provide appropriate actions for the inoperable DG(s).

SURVEILLANCE REQUIREMENTS

As noted at the beginning of the SRs, the SRs for each Unit 2 LOP instrumentation Function are located in the SRs column of Table 3.3.8.1-1. SR 3.3.8.1.5 is applicable only to the Unit 3 LOP instrumentation.

The Surveillance are also modified by a Note to indicate that when a channel is placed in an inoperable status solely for performance of required Surveillance, entry into associated Conditions and Required Actions may be delayed for up to 2 hours provided: (a) for Function 1, the associated Function maintains initiation capability for

(continued)

BASES

SURVEILLANCE REQUIREMENTS (continued)

three DGs; and (b) for Functions 2, 3, 4, 5, the associated Function maintains undervoltage transfer capability for three 4 kV emergency buses. The loss of function for one DG or undervoltage transfer capability for the 4 kV emergency bus for this short period is appropriate since only three of four DGs are required to start within the required times and because there is no appreciable impact on risk. Also, upon completion of the Surveillance, or expiration of the 2 hour allowance, the channel must be returned to OPERABLE status or the applicable Condition entered and Required Actions taken.

SR 3.3.8.1.1 and SR 3.3.8.1.3

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

The Frequency of 31 days is based on operating experience with regard to channel OPERABILITY and drift, which demonstrates that failure of more than one degraded voltage channel of a given Function in any 31 day interval is a rare event. The Frequency of 24 months is based on operating experience with regard to channel OPERABILITY and drift, which demonstrates that failure of the loss of voltage channel in any 24 month interval is a rare event.

SR 3.3.8.1.2

A CHANNEL CALIBRATION is a complete check of the relay circuitry and associated time delay relays. This test verifies the channel responds to the measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drifts between successive calibrations, consistent with the assumptions of the current plant specific setpoint methodology.

The 18 month Frequency for the degraded voltage Functions is based upon the assumption of the magnitude of equipment drift in the setpoint analysis.

(continued)

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.8.1.4

The LOGIC SYSTEM FUNCTIONAL TEST demonstrates the OPERABILITY of the required actuation logic for a specific channel. The system functional testing performed in LCO 3.8.1 and LCO 3.8.2 overlaps this Surveillance to provide complete testing of the assumed safety functions.

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.

SR 3.3.8.1.5

With the exception of this Surveillance, all other Surveillances of this Specification (SR 3.3.8.1.1 through SR 3.3.8.1.4) are applied only to the Unit 2 LOP instrumentation. This Surveillance is provided to direct that the appropriate Surveillance for the required Unit 3 LOP instrumentation are governed by the Unit 3 Technical Specifications. Performance of the applicable Unit 3 Surveillances will satisfy Unit 3 requirements, as well as satisfying this Unit 2 Surveillance Requirement.

The Frequency required by the applicable Unit 3 SR also governs performance of that SR for Unit 2.

REFERENCES

1. UFSAR, Chapter 14.

B 3.3 INSTRUMENTATION

B 3.3.8.2 Reactor Protection System (RPS) Electric Power Monitoring

BASES

BACKGROUND

RPS Electric Power Monitoring System is provided to isolate the RPS bus from the motor generator (MG) set or an alternate power supply in the event of overvoltage, undervoltage, or underfrequency. This system protects the loads connected to the RPS bus against unacceptable voltage and frequency conditions (Ref. 1) and forms an important part of the primary success path of the essential safety circuits. Some of the essential equipment powered from the RPS buses includes the RPS logic and scram solenoids.

RPS electric power monitoring assembly will detect any abnormal high or low voltage or low frequency condition in the outputs of the two MG sets or the alternate power supply and will de-energize its respective RPS bus, thereby causing all safety functions normally powered by this bus to de-energize.

In the event of failure of an RPS Electric Power Monitoring System (e.g., both in series electric power monitoring assemblies), the RPS loads may experience significant effects from the unregulated power supply. Deviation from the nominal conditions can potentially cause damage to the scram solenoids and other Class 1E devices.

In the event of a low voltage condition, the scram solenoids can chatter and potentially lose their pneumatic control capability, resulting in a loss of primary scram action.

In the event of an overvoltage condition, the RPS logic relays and scram solenoids may experience a voltage higher than their design voltage. If the overvoltage condition persists for an extended time period, it may cause equipment degradation and the loss of plant safety function.

Two redundant Class 1E circuit breakers are connected in series between each RPS bus and its MG set, and between each RPS bus and its alternate power supply if in service. Each of these circuit breakers has an associated independent set

(continued)

BASES

BACKGROUND (continued)

of Class 1E overvoltage, undervoltage, underfrequency relays, time delay relays (MG sets only), and sensing logic. Together, a circuit breaker, its associated relays, and sensing logic constitute an electric power monitoring assembly. If the output of the MG set or alternate power supply exceeds predetermined limits of overvoltage, undervoltage, or underfrequency, a trip coil driven by this logic circuitry opens the circuit breaker, which removes the associated power supply from service.

APPLICABLE SAFETY ANALYSES

The RPS electric power monitoring is necessary to meet the assumptions of the safety analyses by ensuring that the equipment powered from the RPS buses can perform its intended function. RPS electric power monitoring provides protection to the RPS components that receive power from the RPS buses, by acting to disconnect the RPS from the power supply under specified conditions that could damage the RPS equipment.

RPS electric power monitoring satisfies Criterion 3 of the NRC Policy Statement.

LCO

The OPERABILITY of each RPS electric power monitoring assembly is dependent on the OPERABILITY of the overvoltage, undervoltage, and underfrequency logic, as well as the OPERABILITY of the associated circuit breaker. Two electric power monitoring assemblies are required to be OPERABLE for each inservice power supply. This provides redundant protection against any abnormal voltage or frequency conditions to ensure that no single RPS electric power monitoring assembly failure can preclude the function of RPS components. Each inservice electric power monitoring assembly's trip logic setpoints are required to be within the specified Allowable Value. The actual setpoint is calibrated consistent with applicable setpoint methodology assumptions.

Allowable Values are specified for each RPS electric power monitoring assembly trip logic (refer to SR 3.3.8.2.2). Trip setpoints are specified in design documents. The trip setpoints are selected based on engineering judgement and operational experience to ensure that the setpoints do not exceed the Allowable Value between CHANNEL CALIBRATIONS. Operation with a trip setting less conservative than the trip setpoint, but within its Allowable Value, is

(continued)

BASES

LCO (continued)

acceptable. A channel is inoperable if its actual trip setting is not within its required Allowable Value. Trip setpoints are those predetermined values of output at which an action should take place. The setpoints are compared to the actual process parameter (e.g., overvoltage), and when the measured output value of the process parameter exceeds the setpoint, the associated device changes state.

The overvoltage Allowable Values for the RPS electrical power monitoring assembly trip logic are derived from vendor specified voltage requirements.

The underfrequency Allowable Values for the RPS electrical power monitoring assembly trip logic are based on tests performed at Peach Bottom which concluded that the lowest frequency which would be reached was 54.4 Hz in 7.5 to 11.0 seconds depending load. Bench tests were also performed on RPS components (HFA relays, scram contactors, and scram solenoid valves) under conditions more severe than those expected in the plant (53 Hz during 11.0 and 15.0 second intervals). Examination of these components concluded that the components functioned correctly under these conditions.

The undervoltage Allowable Values for the RPS electrical power monitoring assembly trip logic were confirmed to be acceptable through testing. Testing has shown the scram pilot solenoid valves can be subjected to voltages below 95 volts with no degradation in their ability to perform their safety function. It was concluded the RPS logic relays and scram contactors will not be adversely affected by voltage below 95 volts since these components will dropout under these voltage conditions thereby satisfying their safety function.

APPLICABILITY

The operation of the RPS electric power monitoring assemblies is essential to disconnect the RPS components from the MG set or alternate power supply during abnormal voltage or frequency conditions. Since the degradation of a nonclass 1E source supplying power to the RPS bus can occur as a result of any random single failure, the OPERABILITY of the RPS electric power monitoring assemblies is required when the RPS components are required to be OPERABLE. This results in the RPS Electric Power Monitoring System OPERABILITY being required in MODES 1 and 2; and in MODES 3, 4, and 5 with any control rod withdrawn from a core cell containing one or more fuel assemblies.

(continued)

BASES (continued)

ACTIONS

A.1

If one RPS electric power monitoring assembly for an inservice power supply (MG set or alternate) is inoperable, or one RPS electric power monitoring assembly on each inservice power supply is inoperable, the OPERABLE assembly will still provide protection to the RPS components under degraded voltage or frequency conditions. However, the reliability and redundancy of the RPS Electric Power Monitoring System is reduced, and only a limited time (72 hours) is allowed to restore the inoperable assembly to OPERABLE status. If the inoperable assembly cannot be restored to OPERABLE status, the associated power supply(s) must be removed from service (Required Action A.1). This places the RPS bus in a safe condition. An alternate power supply with OPERABLE powering monitoring assemblies may then be used to power the RPS bus.

The 72 hour Completion Time takes into account the remaining OPERABLE electric power monitoring assembly and the low probability of an event requiring RPS electric power monitoring protection occurring during this period. It allows time for plant operations personnel to take corrective actions or to place the plant in the required condition in an orderly manner and without challenging plant systems.

Alternately, if it is not desired to remove the power supply from service (e.g., as in the case where removing the power supply(s) from service would result in a scram or isolation), Condition C or D, as applicable, must be entered and its Required Actions taken.

B.1

If both power monitoring assemblies for an inservice power supply (MG set or alternate) are inoperable or both power monitoring assemblies in each inservice power supply are inoperable, the system protective function is lost. In this condition, 1 hour is allowed to restore one assembly to OPERABLE status for each inservice power supply. If one inoperable assembly for each inservice power supply cannot be restored to OPERABLE status, the associated power supply(s) must be removed from service within 1 hour (Required Action B.1). An alternate power supply with OPERABLE assemblies may then be used to power one RPS bus.

(continued)

BASES

ACTIONS

B.1 (continued)

The 1 hour Completion Time is sufficient for the plant operations personnel to take corrective actions and is acceptable because it minimizes risk while allowing time for restoration or removal from service of the electric power monitoring assemblies.

Alternately, if it is not desired to remove the power supply(s) from service (e.g., as in the case where removing the power supply(s) from service would result in a scram or isolation), Condition C or D, as applicable, must be entered and its Required Actions taken.

C.1 and C.2

If any Required Action and associated Completion Time of Condition A or B are not met in MODE 1 or 2, a plant shutdown must be performed. This places the plant in a condition where minimal equipment, powered through the inoperable RPS electric power monitoring assembly(s), is required and ensures that the safety function of the RPS (e.g., scram of control rods) is not required. The plant shutdown is accomplished by placing the plant in MODE 3 within 12 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

D.1

If any Required Action and associated Completion Time of Condition A or B are not met in MODE 3, 4, or 5 with any control rod withdrawn from a core cell containing one or more fuel assemblies, the operator must immediately initiate action to fully insert all insertable control rods in core cells containing one or more fuel assemblies. Required Action D.1 results in the least reactive condition for the reactor core and ensures that the safety function of the RPS (e.g., scram of control rods) is not required.

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS

SR 3.3.8.2.1

A CHANNEL FUNCTIONAL TEST is performed on each overvoltage, undervoltage, and underfrequency channel to ensure that the entire channel will perform the intended function. Any setpoint adjustment shall be consistent with design documents.

As noted in the Surveillance, the CHANNEL FUNCTIONAL TEST is only required to be performed while the plant is in a condition in which the loss of the RPS bus will not jeopardize steady state power operation (the design of the system is such that the power source must be removed from service to conduct the Surveillance). As such, this Surveillance is required to be performed when the unit is in MODE 4 for ≥ 24 hours and the test has not been performed in the previous 184 days. This Surveillance must be performed prior to entering MODE 2 or 3 from MODE 4 if a performance is required. The 24 hours is intended to indicate an outage of sufficient duration to allow for scheduling and proper performance of the Surveillance.

The 184 day Frequency and the Note in the Surveillance are based on guidance provided in Generic Letter 91-09 (Ref. 2).

SR 3.3.8.2.2 and SR 3.3.8.2.3

CHANNEL CALIBRATION is a complete check of the relay circuitry and applicable time delay relays. This test verifies that the channel responds to the measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted between successive calibrations consistent with the plant design documents.

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

SR 3.3.8.2.4

Performance of a system functional test demonstrates that, with a required system actuation (simulated or actual) signal, the logic of the system will automatically trip open the associated power monitoring assembly. Only one signal

(continued)

BASES

SURVEILLANCE REQUIREMENTS

SR 3.3.8.2.4 (continued)

per power monitoring assembly is required to be tested. This Surveillance overlaps with the CHANNEL CALIBRATION to provide complete testing of the safety function. The system functional test of the Class 1E circuit breakers is included as part of this test to provide complete testing of the safety function. If the breakers are incapable of operating, the associated electric power monitoring assembly would be inoperable.

The 24 month Frequency is based on the need to perform this Surveillance under the conditions that apply during a plant outage and the potential for an unplanned transient if the Surveillance were performed with the reactor at power. Operating experience has shown that these components will pass the Surveillance when performed at the 24 month Frequency.

REFERENCES

1. UFSAR, Section 7.2.3.2.

2. NRC Generic Letter 91-09, "Modification of Surveillance Interval for the Electrical Protective Assemblies in Power Supplies for the Reactor Protection System."