7.3 Engineered Safety Feature Systems, Instrumentation and Control

7.3.1 Description

7.3.1.1 Systems Descriptions

This subsection describes the instrumentation and controls for the various engineered safety features (ESF) systems. It provides design basis information as called for by IEEE-603 and provides reference to system diagrams which are included in the ABWR Standard Plant scope.

Supporting systems for the instrumentation and control (I&C) equipment include the instrument, logic, control and motive power sources and are addressed under the heading of “power supplies” for each system.

The ESF systems described in this section include the following:

(1) Emergency Core Cooling Systems (ECCS)

(2) Leak Detection And Isolation System (LDS)

(3) Wetwell And Drywell Spray mode of the RHR System (WDCS-RHR)

(4) Suppression Pool Cooling mode of the RHR System (SPC-RHR)

(5) Standby Gas Treatment System (SGTS)

(6) Emergency diesel generator support systems

(7) Reactor Building Cooling Water (RCW) System and Reactor Service Water (RSW) System

(8) Essential HVAC Systems

(9) HVAC Emergency Cooling Water (HECW) System

(10) High-Pressure Nitrogen Gas Supply (HPIN) System

7.3.1.1.1 Emergency Core Cooling Systems Instrumentation and Controls

The Emergency Core Cooling Systems (ECCS) are a network of the following systems:

(1) High Pressure Core Flooder (HPCF) System

(2) Automatic Depressurization Subsystem (ADS) (SRV electrical activation logic)

(3) Reactor Core Isolation Cooling (RCIC) System

(4) Low-Pressure Flooder (LPFL) mode of the Residual Heat Removal (RHR) System.

The purpose of ECCS instrumentation and controls is to sense the need for ECCS action and to initiate appropriate response from the system in the event of an accident requiring its action.

The ECCS instrument channels detect a need for core cooling systems operation, the logic makes appropriate decisions, and the trip actuators initiate the appropriate equipment operation.

7.3.1.1.1.1 High Pressure Core Flooder System Instrumentation and Controls

(1) System Identification

The I&C components for the HPCF System, except as noted in this subsection, are located outside the drywell. Pressure and level transducers used for HPCF initiation are part of the Nuclear Boiler System and are located on racks outside the drywell. The system is arranged to allow a design flow functional test during normal reactor power operation. The piping and instrumentation diagram (P&ID)is shown in Section 6.3 and the interlock block diagram (IBD)is shown on Figure 7.3-1.

(2) Supporting Systems (Power Supplies)

Supporting systems for the HPCF I&C consist only of the instrumentation, logic and motive power supplies. The controls instrumentation and logic power is obtained from the Class 1E 125 VDC buses (Section 8.3). The logic power is as described in Section 7.2 for the RPS portion of the Reactor Trip and Isolation System (RTIS).

(3) Equipment Design

The HPCF System is designed to operate from preferred offsite power sources or from the Division 2 and 3 diesel generators if offsite (preferred) power is not available.

(a) Initiating Circuits

Reactor vessel water level is monitored by four level transmitters (one in each of the four electrical divisions) that sense the difference between the pressure due to a constant reference leg of water and the pressure due to the actual height of water in the vessel. Each level transmitter provides an input to a remote digital logic controller (RDLC) for analog-to-digital conversion. The formatted, digitized sensor input is transmitted with other sensor signals over an optical fiber data link to the logic processing units in the main control room. All four transmitter signals are fed into the two-out-of-four logic for each of the two divisions (II & III). The initiation logic for HPCF sensors is shown in Figure 7.3-1.

Drywell pressure is monitored by four pressure transmitters in the same four-division configuration described above. Instrument sensing lines that terminate outside the drywell allow the transmitter to communicate with the drywell

interior. Each drywell high-pressure trip channel provides an input into two-out-of-four trip logic shown in Figure 7.3-1.

The HPCF System is initiated on receipt of a reactor vessel low water level signal (Level 1.5) or drywell high-pressure signal from the trip logic. The HPCF System reaches its design flow rate in a time interval consistent with Table 6.3-1. Makeup water is discharged to the reactor vessel until the reactor high water level is reached. The HPCF System then automatically stops flow by closing the injection valve if the high water level signal is available.

This valve will reopen if reactor water level subsequently decreases to the low initiation level. The system is arranged to allow automatic or manual operation. The HPCF initiation signal from the NBS also initiates the standby diesels in the respective divisions.

An AC motor-operated valve and a check valve are provided in both branches of the pump suction. The pump suction can be aligned through one branch to the condensate storage tank or aligned through the other branch to the suppression pool. The control arrangement is shown in Figure 7.3-1. Reactor grade water in the condensate storage tank is the preferred source. On receipt of an HPCF initiation signal, the condensate storage tank suction valves are automatically signaled to open unless the suppression pool suction valves are fully open. If the water level in the condensate storage tank falls below a preselected level, first the suppression pool suction valves automatically open and then the condensate storage tank suction valves automatically close. Four level transducers (one in each electrical division) are used to detect low water level in the condensate storage tank. Any two-out-of-four transducers can cause the suppression pool suction valves to open and the condensate storage tank valves to close. The suppression pool suction valves also automatically open if high water level is detected in the suppression pool. Four level transducers (one in each electrical division) monitor this water level and two-out-of-four transducers can initiate opening of the suppression tank suction valves and closure of condensate storage tank suction valves.

(b) Logic and Sequencing

Either reactor vessel low water level (Level 1.5) or high drywell pressure automatically starts the HPCF System (Figure 7.3-1).

(c) Bypasses and Interlocks

The HPCF pump motors and injection valves are provided with manual override controls which permit the operator manual control of the system following a LOCA.

During test operation, the HPCF pump discharge is routed to the suppression pool. Two motor-operated valves are installed in the test lines for each loop. The piping arrangement is shown in Figure 6.3-1. The control scheme for the valves is shown in Figure 7.3-1. On receipt of an HPCF initiation signal, the test line valves close and remain closed.

The HPCF pump is interlocked with a corresponding bus undervoltage monitor. The pump motor circuit breaker will not close unless the voltage on the bus supplying the motor is above the setpoint of the undervoltage monitor.

(d) Redundancy and Diversity

The HPCF System is actuated by reactor vessel low water level (Level 1.5) or drywell high pressure. Both of these conditions may result from a design basis loss-of-coolant accident.

The HPCF System logic requires any two of the four independent reactor vessel water level measurements to concurrently indicate the high water level (Level 8) condition. When the high water level condition is reached following HPCF operation, these two signals are used to stop HPCF flow to the reactor vessel by closing the injection valve. However, the pump continues to run unless deliberately stopped by the operator with the pull-to-lock switch. Should the low water level (Level 1.5) condition recur, the injection valve will reopen automatically. This action will restore water level within the reactor unless the operator has used the pull-to-lock stop of the pump motor due to HPCF loop failure (i.e., ruptured injection line, etc.). In that event, adequate water level is assured with the redundant HPCF and RCIC divisions and, if necessary, the ADS and low pressure flooder mode of the RHR. The locked-out loop can be manually restarted by unlocking the switch and placing it in the START position.

For additional diverse HPCF features to mitigate potential common-mode failure conditions, see the discussion in Subsection 7C.5.

(e) Actuated Devices

All motor-operated valves in the HPCF System are equipped with remote-manual functional test feature. The entire system can be manually operated from the main control room.

Motor-operated valves are provided with limit switches to turn off the motor when the full open or closed positions are reached. Torque switches also control valve motor forces while the valves are seating.

The HPCF valves must be opened sufficiently to provide design flow rate within the time interval consistent with Table 6.3-1.

The HPCF pump discharge line is provided with an AC motor-operated injection valve. The control scheme for this valve is shown in Figure 7.3-1. The valve opens on receipt of the HPCF initiation signal. The pump injection valve closes automatically on receipt of a reactor high water level (Level 8) signal.

Two pressure transmitters and associated control room interfaces are installed in each pump discharge pipeline to verify that pumps are operating following an initiation signal. The pressure signals are used in the Automatic Depressurization Subsystem to verify availability of high pressure core cooling.

(f) Separation

Separation within the ECCS is such that no single design basis event, in conjunction with an additional single failure, can prevent core cooling when required. Control and electrically driven equipment wiring is segregated into three separate electrical divisions, designated I, II and III (Figure 8.3-1). Initiation sensor inputs are from all four divisions. HPCF is a two-division system utilizing Divisions II and III. HPCF control logic, cabling, manual controls and instrumentation are arranged such that divisional separation is maintained. System separation and diesel loading are shown in Table 8.3-1.

(g) Testability

The high-pressure core flooder (HPCF) instrumentation and control system is capable of being tested during normal unit operation to verify the operability of each system component. Testing of the initiation transmitters which are located outside the drywell is accomplished by valving out each transmitter, one at a time, and applying a test pressure source. This verifies the operability of the transmitter, as well as the calibration range. The analog sensor inputs are calibrated at the analog inputs of the RDLCs. With a division-of-sensors bypass in place, calibrated, variable signals are injected in place of the sensor signals and monitored at the ELCS control room panels for linearity, accuracy, fault response, and downscale and upscale trip response.

Testing for functional operability of the control logic is accomplished as discussed in Subsection 7.1.2.1.6.

Availability of the other control equipment is verified during manual testing of the system with the pump discharge returning to the suppression pool. A design flow functional test of the HPCF System may be performed during normal

plant operation by drawing suction from the suppression pool and discharging through a full flow test return line to the suppression pool.

(h) Environmental Considerations

The only HPCF System I&C components located inside the drywell are the control mechanism and valve position switches for the testable check valve and bypass valves on the pump discharge lines, and maintenance valve position switches. All other HPCF I&C equipment are located outside the drywell and is selected to meet the environmental requirements presented in Section 3.11.

(i) Operational Considerations

Under abnormal or accident conditions where the system is required, initiation and control are provided automatically. Operator action may be initiated at any time, but is not necessary after automatic initiation.

Pressure in the HPCF pump suction line is monitored by a pressure transmitter to permit the determination of suction head and pump performance. Numerous other indications pertinent to the operation and condition of the HPCF system are available to the control room operator as shown in Figures 6.3-1 (HPCF P&ID) and 7.3-1 (HPCF IBD).

Chapter 16 describes the methods for calculating setpoints and margins.

(j) Parts of System Not Required for Safety

The non-safety-related portions of the HPCF System include the annunciators and the plant computer functions (PCFs). Other instrumentation considered non-safety-related are those indicators which are provided for operator information but are not essential to correct operator action.

7.3.1.1.1.2 Automatic Depressurization Subsystem Instrumentation and Controls

(1) System Identification

Automatic safety/relief valves (SRVs) are installed on the main steamlines inside the drywell. The valves can be actuated in two ways: (1) by pneumatic action or (2) by mechanical actuation without power. The suppression pool provides a heat sink for steam relieved by these valves. Relief valve operation may be controlled manually from the control room to hold the desired reactor pressure. Eight of the SRVs are designated as Automatic Depressurization Subsystem (ADS) valves and are capable of operating from either ADS logic or safety/relief logic signals. The safety/relief logic is discussed in Paragraph (4). Automatic depressurization by the ADS is provided to reduce the pressure during a loss-of-coolant accident in which the HPCF

and RCIC Systems are unable to restore vessel water level. This allows makeup of core cooling water by the low pressure makeup system (RHR/LP flooding mode).

(2) Supporting System (Power Supplies)

Supporting systems for the ADS include the instrumentation, logic, control and motive power sources. The instrumentation and logic power and control power is from the Division I and II, 125 VDC battery buses (see Figure 8.3-4). The motive power for the electrically operated gas pilot solenoid valves is from local accumulators supplied by the High Pressure Nitrogen Gas Supply System (Divisions I and II) (see Section 6.7).

(3) Equipment Design

The Automatic Depressurization Subsystem (ADS) consists of redundant trip channels arranged in two separate logics that control two separate solenoid-operated gas pilots on each ADS valve. Either pilot valve can operate its associated ADS valve. These pilot valves control the pneumatic pressure applied by accumulators and the High-Pressure Nitrogen Gas Supply System. The operator can also control the SRVs manually. Separate accumulators are included with the control equipment to store pneumatic energy for relief valve operation.

The ADS accumulators are sized to operate the SRV one time at drywell design pressure or five times at normal drywell pressure, following failure of the pneumatic supply to the accumulator. Sensors provide inputs to an RDLC for analog-to-digital conversion. The formatted, digitized sensor inputs are transmitted with other sensor signals over an optical data link to the logic processing units in the main control room. All four transmitter signals are fed into the two-out-of-four logic for each of two divisions, either of which can actuate the ADS. Station batteries and ELCS power supplies energize the electrical control circuitry. The power supplies for the redundant divisions are separated to limit the effects of electrical failures. Electrical elements in the control system energize to cause the relief valves to open.

(a) ADS Initiating Circuits

Two ADS subsystems (ADS 1 and ADS 2) for relief valve actuation are provided (Figure 7.3-2). Sensors from all four divisions and Division I control logic for low reactor water level and high drywell pressure initiate ADS 1, and sensors from all four divisions and Division II control logic initiate ADS 2. The Division I logic is mounted in a different cabinet than the Division II logic.

The reactor vessel low water level initiation setting for the ADS is selected to depressurize the reactor vessel in time to allow adequate cooling of the fuel by the RHR (LP flooding mode) System following a LOCA in which the HPCF and/or RCIC Systems fail to perform their functions adequately. Timely

depressurization of the reactor vessel is provided if the reactor water level drops below acceptable limits, together with an indication that high drywell pressure has occurred, which signifies there is a loss of coolant into the containment with insufficient high pressure makeup to maintain reactor water level. For breaks outside the containment, timely depressurization of the reactor vessel is provided if the reactor vessel water level drops below acceptable limits for a time period sufficient for the ADS high drywell pressure bypass timer and the ADS timer to time-out. Reactor isolation occurs on loss of coolant outside the containment.

The HPCF and RHR-LPFL discharge pressure settings are used as a permissive for depressurization and are selected to assure that at least one of the three RHR pumps, or one of the two HPCF pumps, has received electrical power, started, and is capable of delivering water into the vessel. The pressure setting is high enough to assure that the pump will deliver at or near rated flow without being so high as to fail to show that the pump is actually running.

The level transmitters used to initiate one ADS logic are separated from those used to initiate the other ADS logic. Reactor vessel low water level is detected by eight transmitters that measure differential pressure. Drywell high pressure is detected by four pressure transmitters. All the vessel level and drywell high-pressure transmitters are located in the Reactor Building outside the drywell. The drywell high-pressure signals are arranged to seal-in the control circuitry. They must be manually reset to clear.

Time delay logic is used in each ADS control division. The time delay setting before actuation of the ADS is long enough that the HPCF and/or RCIC System has time to restore water level, if capable, yet not so long that the RHR (LPFL-mode) System is unable to adequately cool the fuel if the HPCF System fails to prevent low water level. An annunciator in the control room is actuated when either of the timers is timing. Resetting the ADS initiating signals has no effect on the timers if the initiating signals are still present.

If the reactor level is restored sufficiently to reset the previous actuation setpoints before the timer times out, the timer automatically resets and auto-depressurization is aborted. Should additional level dips occur across the setpoints, the timer resets with each one.

For anticipated transient without scram (ATWS) mitigation, the ADS has an automatic and manual inhibit of the automatic ADS initiation. The average power range monitors (APRMs) ATWS permissive signal is combined with the reactor water level signal (Level 1.5) such that ADS automatic initiation is inhibited unless both power and level are below their setpoints. There are main control room switches for the manual inhibit of automatic initiation of ADS.

(b) Logic and Sequencing

Two parameters of initiation signals are used for the ADS: drywell high pressure and reactor vessel water below Level 1 or reactor vessel water below Level 1 alone after a time delay. Two-out-of-four of each set of signals must be present throughout the timing sequence to cause the SRVs to open. Each parameter separately seals itself in and annunciates following the two-out-of-four logic confirmation. Low Water Level 1 is the final sensor to initiate the ADS.

A permissive signal of RHR (LP flooder mode) or HPCF pump discharge pressure is also used. Discharge pressure on any one of the three RHR pumps or one of the two HPCF pumps is sufficient to give the permissive signal which permits automatic depressurization when the RHR or HPCF System is operable.

After receipt of the initiation signals and after a delay provided by time delay elements, each of the two solenoid pilot gas valves is energized. This allows pneumatic pressure from the accumulator to act on the gas cylinder operator. The gas cylinder operator opens and holds the relief valve open. Lights in the main control room indicate when the gas cylinder operator is a safety/relief valve. Limit switches mounted on the gas cylinder operators verify each valve position to the plant computer function (PCF) and the annunciators.

The ADS Division I control logic actuates a solenoid pilot valve on each ADS valve. Similarly, the ADS Division II control logic actuates a second separate solenoid pilot valve on each ADS valve. Actuation of either solenoid-pilot valve causes the ADS valve to open to provide depressurization.

Manual reset circuits are provided for the ADS initiation signal and the two parameter sensor input logic signals. An attempted reset has no effect if the two-out-of-four initiation signals are still present from each parameter (high drywell pressure and reactor water below Level 1). However, an inhibit switch is provided for each division which can be used to take one ADS division out of service for testing or maintenance during plant operation. This switch is ineffective once the ADS timers have timed out and thus cannot be used to abort and reclose the valves once they are signalled to open. The inhibit mode is continuously annunciated in the main control room.

Manual actuation pushbuttons are provided to allow the operator to initiate ADS immediately (no time delay) if required. Such initiation is performed by first rotating the collars surrounding the pushbuttons for each of two channels within one of the two divisions. An annunciator will sound to warn the operator that the ADS is armed for that division. If the two pushbuttons are then

depressed, the ADS valves will open, provided the ECCS pump(s) running permissives are present. Though such manual action is immediate, the rotating collar permissives and duality of button sets combined with annunciators assure manual initiation of the ADS to be a deliberate act.

A control switch is available in the main control room for each SRV, including the ones associated with the ADS. Each switch is associated with one SRV. The eighteen SRVs are divided into three groups of six for pressure relief operation and are powered by Division I, II or III of the Class 1E 125 VDC busses. The three electrical divisions maintain electrical separation consistent with the required operability, though its function is not required for safety. The switches are three-position keylock-type, OFF-AUTO-OPEN, located on the main control board. The OPEN position is for manual SRV operation. Manual opening of the relief valves provides a controlled nuclear system cooldown under conditions where the normal heat sink is not available.

For anticipated transient without scram (ATWS) mitigation, the ADS has an automatic and manual inhibit of the automatic ADS initiation. The average power range monitors (APRM) ATWS permissive signal is combined with the reactor water level signal (Level 1.5) such that ADS automatic initiation is inhibited unless both power and level are below their setpoints.. There are main control room switches for the manual inhibit of automatic initiation of ADS.

(c) Bypasses and Interlocks

There is one manual ADS inhibit switch in the control room for each ADS logic and control division which will inhibit ADS initiation, if ADS has not initiated. The primary purpose of the inhibit switch is to remove one of the two ADS logic and control divisions from service for testing and maintenance during plant operation. The ADS is interlocked with the HPCF and RHR Systems by means of pressure sensors located on the discharge of these pumps. Manual ADS bypasses the timers and immediately opens the ADS valves, provided the ECCS pump(s) running permissives are present. The need to rotate the collar before depressing the pushbutton, combined with annunciators, assure manual initiation of ADS to be a deliberate act.

(d) Redundancy and Diversity

The ADS is initiated by high drywell pressure and/or reactor vessel water below Level 1. The initiating circuits for each of these parameters are redundant as described by the circuit description of this section. Diversity is provided by the HPCF and RCIC Systems.

(e) Actuated Devices

Safety/relief valves are actuated by any one of four methods:

(i) ADS Action

Automatic action after high drywell pressure followed by 29 seconds at low water level (L1) or low water level (L1) for 8 minutes (ADS high drywell pressure bypass timer) and 29 seconds (ADS timer), plus makeup pumps running, resulting from the logic chains in either Division I or Division II control logic actuating.

(ii) Manual

Manual action by the operator (either by ADS system level actuation, or by individual SRV operating switches).

(iii) Pressure Relief Action

Pressure transmitter signals above setpoints as a result of high reactor pressure (Paragraph (4)).

(iv) Safety/Relief Action

Mechanical actuation as a result of high reactor pressure (higher than pressure in item iii).

(f) Separation

Separation of the ADS is in accordance with criteria stated in Section 7.1. ADS is a Division I (ADS 1) and Division II (ADS 2) system, except that only one set of relief valves is supplied. Each ADS relief valve can be actuated by any one of three solenoid pilot valves supplying nitrogen gas to the relief valve gas piston operators. One of the ADS solenoid pilot valves is operated by Division I logic and the other by Division II logic. The third solenoid pilot is used for non-ADS operation. The non-ADS SRV function solenoid pilot valves are powered from Division I, II, or III Class 1E DC bus. Control logic manual controls and instrumentation are mounted so that Division I and Division II separation is maintained. Separation from Divisions III and IV is likewise maintained.

(g) Testability

The ADS has two complete control logics, one in Division I and one in Division II. Each control logic has two circuits, both of which must operate to initiate ADS. Both circuits contain time delay logic to give the HPCF System an opportunity to restore water level. The ADS instrument channels signals are verified by cross comparison between the channels which bear a known relationship to each other. Indication for each instrument channel is available

on displays associated with the ELCS. SSLC testing, as described in the sixth test, discussed in Subsection 7.1.2.1.6 is also applicable here for the ADS. The instrument channels are manually verified in accordance with Technical Specification requirements. Testing of ADS does not interfere with automatic operation if required by an initiation signal. The pilot solenoid valves can also be tested.

(h) Environmental Considerations

The signal cables, solenoid valves, SRV operators and accumulators, and RV water level instrument lines are the only essential I&C equipment for the ADS located inside the drywell. These items will operate in the most severe environment resulting from a design basis LOCA (Section 3.11). Gamma and neutron radiation is also considered in the selection of these items. Equipment located outside the drywell (viz., the RPV level and DW pressure transmitters and data communication interfaces) will also operate in their normal and accident environments.

(i) Operational Considerations

The instrumentation and controls of the ADS are not required for normal plant operations. When automatic depressurization is required, it will be initiated automatically by the circuits described in this section. No operator action is required for at least 30 minutes following initiation of the system.

A temperature element is installed on the SRV discharge piping several feet from the valve body. The temperature element provides input to the historian function in the control room to provide a means of detecting SRV leakage during plant operation. When the temperature in any SRV discharge pipeline exceeds a preset valve, an alarm is sounded in the main control room. The alarm setting is enough above normal rated power drywell ambient temperatures to avoid spurious alarms, yet low enough to give early indication of SRV leakage.

Chapter 16 describes the methods for calculating setpoints and margins.

(j) Parts of System Not Required for Safety

The non-safety-related portions of the ADS include the annunciators and the PCF. Other instrumentation considered non-safety-related are those indicators which are provided for operator information, but are not essential to correct operator action.

(4) Pressure Relief Function of the Safety/Relief Valves

The nuclear pressure relief system is designed to prevent overpressurization of the nuclear system that could lead to the failure of the reactor coolant pressure boundary. Details of the design bases are discussed in Subsection 5.2.2. Pressure relief of the Nuclear Boiler System (Figure 7.3-2) is by spring-release mechanical actuation of all the SRVs, including the valves used in the automatic depressurization function. In addition, all SRVs have power actuators that also open the valves and limit valve closing forces. The electrical power actuation function for non-ADS SRVs is not required for safety.

All SRVs have individual non-safety-related accumulators. In addition, those with ADS function each have a separate safety-related larger capacity accumulator with separate redundant gas power actuators. The SRVs are initiated by reactor vessel pressure, which is monitored by Class 1E transmitters within each of the four divisions. These transmitters are not dedicated to the SRV logic but are shared with other I&C systems in common with respective division. Trip signals from all four divisions are combined through optical isolators in two-out-of-four logic such that two or more signals are required to electrically actuate each relief valve. Each valve actuator is powered from Division I, II or III of the station Class 1E 125 VDC buses. The power interfaces are distributed among the four divisions for the 18 SRVs.

7.3.1.1.1.3 Reactor Core Isolation Cooling (RCIC) System—Instrumentation and Controls

(1) Function

The instrumentation and controls (I&C) for the Reactor Core Isolation Cooling (RCIC) System provide control for the pump/turbine valves, and accessories during the following conditions:

(a) A loss-of-coolant accident (LOCA) event.

(b) When the reactor vessel is isolated and yet maintained in the hot standby condition.

(c) When the reactor vessel is isolated and accompanied by a loss of normal coolant flow from the reactor feedwater system.

(d) When a complete plant shutdown under conditions of loss of normal feedwater is started before the reactor is depressurized sufficiently for the reactor shutdown cooling mode of the RHR System to placed into operation.

(e) Should a complete loss of AC power occur, the RCIC System is designed to operate for at least 30 minutes for these conditions.

(2) Classification

The RCIC System is classified as a safety-related system and is designed to assure that sufficient reactor water inventory is maintained in the reactor vessel to permit adequate core cooling to take place.

(3) Power Sources

The RCIC System is primarily powered by the Division I 125 VDC system. Exceptions include the inboard isolation valves (including the steam line warm-up valve) which are powered by 480 VAC Division I and the outboard steam supply isolation valve is powered by 125 VDC Division II. The logic power is as described in Section 7.1 for ELCS.

(4) Equipment

When actuated, the RCIC System pumps demineralized water from the condensate storage tank to the reactor vessel. The suppression pool provides an alternate source of water. The RCIC System includes a 100% capacity steam-driven turbine which drives a 100% capacity pump assembly, turbine and pump accessories, piping, valves, and instrumentation necessary to implement several flow paths. The arrangement of equipment and control devices is shown in Figure 5.4-8 (RCIC P&ID).

Level transmitters used for the initiation and stopping RCIC are provided by the Nuclear Boiler System and are shared by other system channels within each division. High drywell pressure signals are provided by the Nuclear Boiler System and are also shared by other system channels within each division. These are located outside the drywell but inside the Reactor Building. The only operating components of the RCIC System that are located inside the drywell are the inboard steamline isolation valve and the steamline warmup line isolation valve.

The rest of the RCIC System normal I&C components are located in the Reactor Building. Cables connect the sensors (via the Essential Communication Function) to control circuitry in the main control room.

A design flow functional test of the RCIC System may be performed during normal plant operation by drawing suction from the suppression pool and discharging through a full flow test return line to the suppression pool. The discharge valve to the reactor vessel remains closed during the test and reactor operation remains undisturbed. All components of the RCIC System except for the RCIC injection line stop valve are capable of individual functional testing during normal plant operation.

Control system decisions will provide automatic return from test to operating mode if RCIC System initiation is required. There are two exceptions:

(i) Not Used

(ii) Steam inboard/outboard isolation valves are closed. Closure of either or both requires operator action to properly sequence their opening.

(iii) Breakers have been manually racked out of service. This condition is indicated in the main control room.

(a) Initiating Circuits

The RCIC System is initiated upon receipt of a high drywell pressure signal or a reactor vessel low water Level 2 signal. High drywell pressure is monitored by four shared pressure transmitters (one from each division) in the Nuclear Boiler System. Reactor vessel low water level is monitored by four shared level transmitters (one from each of the four electrical divisions) in the NBS that sense the pressure difference between a constant reference leg of water and the actual height of water in the vessel.

Each transmitter supplies a signal for analog-to-digital conversion. The formatted, digitized sensor inputs are transmitted with other sensor signals over an optical data link to the logic processing units in the main control room. All four transmitter signals are fed into the two-out-of-four logic for RCIC initiation.

The sensing lines for the transmitters are physically separated from each other and tap off the reactor vessel at each of the four quadrants of the containment structure associated with the appropriate electrical divisions.

The RCIC System is initiated automatically after receipt of either of the two parameters just described and produces the design flow rate in a time interval consistent with Table 6.3-1. The system then functions to provide design makeup water flow to the reactor vessel until the amount of water delivered to the reactor vessel is adequate to restore vessel level. The RCIC turbine will shut down automatically upon receipt of high reactor water level (two-out-of-four). The controls are arranged to allow manual startup, operation, and shutdown.

The RCIC turbine is functionally controlled by an internal turbine flow controller. The turbine governor limits the turbine speed and adjusts the turbine steam inlet so that design pump discharge flow rate is obtained. The flow signal used for automatic control of the turbine is derived from a differential pressure measurement within the turbine. All flow controls are internal to the combined turbine pump.

The turbine is automatically shut down by tripping the turbine and closing the throttle valve if any of the following conditions are detected:

(i) Turbine overspeed
(ii) High turbine exhaust pressure
(iii) RCIC auto-isolation signal
(iv) Low pump suction pressure
(v) Reactor vessel high water level (Level 8)
(vi) Manual trip activated by the operator

Turbine overspeed indicates a malfunction of the turbine control mechanism. High turbine exhaust pressure indicates an obstruction in the exhaust line. Low pump suction pressure warns that cavitation and lack of cooling can cause damage to the pump which could place it out of service. RCIC shutdown is initiated for these conditions so that if the causes of the abnormal conditions can be found and corrected, the system can be quickly restored to service. Turbine overspeed is first detected by an electrical overspeed sensor, and secondly by a throw-out pin overspeed mechanical device. High turbine exhaust pressure can initiate turbine shutdown. Two pressure sensors can be used to detect low RCIC System pump suction pressure (only one of these need to function since the logic is structured such that one can be in calibration at any time).

RCIC is automatically isolated on detection of high steam flow or high temperature in the RCIC room. Either of these is an indication of a steam line leak or break.

High water level in the reactor vessel indicates that the RCIC System has performed satisfactorily in providing makeup water to the reactor vessel. A further increase in level could result in steam line damage caused by gross carryover of moisture. The reactor vessel high water Level 8 setting which stops the turbine is below the bottom of the Main Steam Line (MSL) and is selected to prevent overflow into the MSLs. Four shared level transmitters from the Nuclear Boiler System which sense differential pressure are arranged in two-out-of-four logic to initiate a turbine shutdown. However, should a subsequent low level signal recur, the RCIC System will automatically restart.

(b) Logic and Sequencing

The scheme used for initiating the RCIC System is shown in Figure 7.3-3 (RCIC IBD). RCIC initially starts on the sensing of either a low water level (Level 2) signal or a high drywell pressure signal. This initiates a sequence of valve openings and a RCIC turbine ramp rate which results in rated flow to the reactor vessel in a time interval consistent with Table 6.3-1.

About 5 seconds after the initiation signal is received, the RCIC steam admission valve opens. The RCIC turbine controller controls the flow ramp rate to rated flow to the reactor vessel.

(c) Bypasses and Interlocks

To prevent the turbine/pump from being damaged by overheating at reduced RCIC pump discharge flow, a pump minimum flow bypass is provided to route the water discharged from the pump back to the suppression pool.

The minimum flow bypass is controlled by an automatic DC motor-operated valve. The control scheme is shown in Figure 7.3-3 (RCIC IBD). The valve is automatically closed at high flow or when either the admission steam supply valve or turbine trip valves are closed. Low flow, combined with high pump discharge pressure, opens the valve.

To prevent the RCIC steam supply pipeline from filling up with water, a condensate drain pot, steamline drain, and appropriate valves are provided in a drain pipeline arrangement just upstream of the turbine supply valve. During normal operation, steamline drainage is routed to the main condenser. The water level in the steamline drain condensate pot is controlled by a steam trap. If above normal condensation occurs, as is typical during initial steam line warm up, a level switch and a direct acting solenoid valve energize to allow condensate to flow out of the drain pot, bypassing the normal steam trap. This condition is alarmed in the MCR.. Upon receipt of an RCIC initiation signal and subsequent opening of the steam admission supply valve, this drainage path is shut off by redundant valves.

To prevent the turbine exhaust line from filling with water, a condensate drain pot is provided to route the turbine exhaust line to a drain tank. RCIC initiation and subsequent opening of the steam admission supply valve causes the exhaust drainage line to be shut off by redundant valves.

During Full Flow Test Mode operation, the RCIC pump discharge is routed to the suppression pool. Two DC motor-operated valves are installed in the pump discharge to the suppression pool pipeline. The piping arrangement is shown in Figure 5.4-8 (RCIC P&ID). Upon receipt of an RCIC initiation signal while in the Full Flow Test Mode, the RCIC pump discharge valves and CST suction valve close and the suction remains aligned to the suppression pool during this transition to the Vessel Makeup Mode. The RCIC pump suction may be remotely realigned to the CST, as shown in Figure 7.3-3 (RCIC IBD). Various indications pertinent to the operation and condition of the RCIC System are available to the main control room operator. Figure 7.3-3 (RCIC IBD) shows the various indications provided.

(d) Redundancy and Diversity

On a network basis, the HPCF System is redundant and diverse to the RCIC System for the ECCS and safe shutdown function. Therefore, the RCIC System, as a system by itself, is not required to be redundant or diverse, although the instrument channels are redundant for operational availability purposes.

The RCIC System is actuated by high drywell pressure or by reactor low water level (Level 2). Four NBS sensors monitor each parameter and combine in two sets of two-out-of-four logic signals in the ESF Logic and Control System (ELCS). A permissive signal from either set initiates the RCIC System. The sensor outputs themselves are shared by other systems in common with each division.

(e) Actuated Devices

All automatic valves in the RCIC System are equipped with remote manual test capability so that the entire system can be operated from the control room. Motor-operated valves are equipped with limit and torque switches. Limit switches turn off the motors when movement is complete. In the closing direction, torque switches turn the motor off when the valve has properly seated. Thermal overload devices are used to trip motor-operated valves during testing only (for more information on valve testing, see Subsection 3.9.3.2). All motor-operated and air-operated valves provide control room indication of valve position. RCIC is capable of initiation independent of AC power.

To assure that the RCIC System can be brought to design flow rate in an time interval consistent with Table 6.3-1 from receipt of the initiation signal, the following maximum operating times for essential RCIC valves are provided by the valve operation mechanisms:

– RCIC turbine steam admission supply valve: 15 s

– RCIC pump discharge valves: 15 s

– RCIC pump minimum flow bypass valve: 5 s

The operating time is the time required for the valve to travel from the fully-closed to the fully-open position or vice versa. A normally closed steam admission supply valve is located in the turbine steam supply pipeline just upstream of the turbine stop valve. The control scheme for this valve is shown in Figure 7.3-3 (RCIC IBD). Upon receipt of an RCIC initiation signal this valve opens and remains open until closed by a high water level signal, or by operator action from the main control room.

Two normally open isolation valves, one inboard and one outboard, are provided in the steam supply line to the turbine. These valves automatically close upon receipt of an RCIC isolation signal. The inboard isolation valve has a bypass line with an automatic remotely controlled valve in it. The bypass line is used to equalize and preheat the steamline to the RCIC steam admission supply valve.

The signals for isolation are provided by the Leak Detection and Isolation System (LDS) and consist of the following:

– **Outboard RCIC turbine isolation valve:**

(i) Ambient temperature sensors—RCIC equipment area B high temperature.

(ii) Not Used

(iii) RCIC flow instrument line B break or high flow.

(iv) Two pressure transmitters and trip logic—RCIC turbine exhaust high pressure. Both trip logic channels must activate to isolate.

(v) Pressure transmitter and trip logic RCIC steam supply pressure low.

(vi) RCIC manual isolation Channel B.

– **Inboard RCIC turbine isolation valve:**

The same set of two-out-of-four logic causes the inboard valve to isolate, except manual isolation is a separate control in Division I.

Two pump suction valves are provided in the RCIC System. One valve lines up pump suction from the condensate storage tank, the other one from the suppression pool. The condensate storage tank is the preferred source. The control arrangement is shown in Figure 7.3-3 (RCIC IBD). Upon receipt of an RCIC initiation signal, the condensate storage tank suction valves are automatically signaled to open unless the suppression pool suction valves are fully open. Condensate storage tank low water level or suppression pool high water level automatically opens the suppression pool suction valve. Full opening of this valve automatically closes the condensate storage tank suction valve.

One RCIC pump discharge valve and two check valves are provided in the pump discharge pipeline. The control scheme for the discharge valve is shown in Figure 7.3-3 (RCIC IBD). This discharge valve is arranged to open upon receipt of the RCIC initiation signal and closes automatically upon closure of the turbine stop valve or the RCIC steam admission supply valve.

(f) Separation

The RCIC System is basically a Division I system but includes both Division I and Division II valves for isolation. Therefore, part of the RCIC logic (the outboard isolation logic) is Division II. In order to maintain the required separation, RCIC trip channel and logic components, instruments, and manual controls are mounted so that separation from Division II is maintained.

All power and signal cables and cable trays are clearly identified by division and safety classification.

(g) Testability

The RCIC System may be tested to design flow during normal plant operation. The system is designed to return to the operating mode if system initiation is required during testing. Water is drawn from the suppression pool and discharged through a full flow test return line to the suppression pool. The discharge valve from the pump to the reactor is tested separately and closed during the system flow test so that reactor operation remains undisturbed.

Verification of sensor signals is accomplished by cross comparison between the redundant channels. Each sensor signal is monitored on the ELCS and Main Control Room (MCR) displays. Additional testing of the initiation sensors which are located outside the drywell may be accomplished by valving out each sensor and applying a test pressure source. This verifies the calibration range in addition to the operability of the sensor. The logic is manually verified in accordance with Technical Specification Requirements. SSLC testing as discussed in Subsection 7.1.2.1.6 is also applicable here for the RCIC System.

(5) Environmental Considerations

The only RCIC control components located inside the drywell that must remain functional in the environment resulting from a loss-of-coolant accident are the control mechanisms for the inboard isolation valve and the steamline warmup line isolation valve. The RCIC I&C equipment located outside the drywell is selected in consideration of the environments in which it must operate. All safety-related RCIC instrumentation is seismically qualified to remain functional following a safe shutdown earthquake (SSE) (Section 3.10).

(6) Operational Considerations

Normal core cooling is required in the event that the reactor becomes isolated from the main condenser during normal operation by a closure of the main steamline isolation valves. Cooling is necessary due to the core fission product decay heat.

Steam pressure is relieved through the SRVs to the suppression pool. Under these conditions, RCIC maintains reactor water level by providing the makeup water. Initiation and control are automatic.

The following indications are available in the main control room for operator information:

RCIC steamline supply pressure

RCIC valve (test bypass to suppression pool) position

RCIC pump discharge pressure

RCIC pump discharge flow

RCIC turbine speed

RCIC turbine exhaust line pressure

Position of motor-operated valves

Turbine trip

System status (power, test, isolation)

Annunciators

(7) Setpoints

The reactor vessel low water Level 2 setting for RCIC System initiation is selected high enough above the active fuel to start the RCIC System in time to prevent the need for the use of the low pressure ECCS. The water level setting is far enough below normal levels that spurious RCIC System startups are avoided. Chapter 16 describes the methods for calculating the setpoints and margins.

7.3.1.1.1.4 RHR/Low Pressure Flooder (LPFL) Instrumentation and Controls

(1) System Identification

The Low Pressure Flooder (LPFL) Subsystem is an operating mode of the Residual Heat Removal (RHR) System (RHR System and its operating modes are discussed in Chapter 5). Because the LPFL Subsystem is designed to provide water to the reactor vessel following the design basis LOCA, its controls and instrumentation are discussed here.

(2) Supporting Systems (Power Supplies)

Supporting systems for the LPFL Subsystem include only the instrumentation, control and motive power supplies. Divisions I, II, and III are used for the three loops of the LPFL.

(3) Equipment Design

Figure 5.4-10 (RHR P&ID) shows the entire RHR System, including the equipment used for LPFL operation. Control and instrumentation required for the operation of the LPFL mode are safety-related.

The instrumentation for LPFL operation controls all necessary valves in the RHR System. This ensures that the water pumped from the suppression pool by the main system pumps is routed directly to the reactor. These interlocking features are described in this subsection.

LPFL operation uses three pump loops, each loop with its own separate vessel injection path. Figure 5.4-10 (RHR P&ID) shows the location of instruments, control equipment, and LPFL components. Except for the shutdown cooling inboard suction isolation valves and the testable check valves for Divisions II and III, the components pertinent to LPFL operation are located outside the drywell.

Motive power for the RHR System pumps is supplied from AC buses that can receive standby AC power. The three pumps are powered from Division I, II, and III ESF buses, which also provide power to the RCIC (Division I) and HPCF (Divisions II and III) Systems. Motive power for the automatic valves comes from the bus that powers the pumps for that division, except for the special case involving isolation valves. Control power for the LPFL Subsystem components comes from the divisional Class 1E AC buses. Logic power is from the ELCS power supply for the division involved. Trip channels for the LPFL Subsystem are shown in Figure 7.3-4.

The LPFL Subsystem is arranged for automatic and remote-manual operation from the control room.

(a) Initiating Circuits

The LPFL Subsystem is initiated automatically on receipt of a high drywell pressure or low reactor water level signal (Level 1), and a low reactor pressure permissive to open the injection valve. The LPFL may also be initiated manually.

Reactor vessel low water Level 1 is monitored by four level transmitters from the Nuclear Boiler System (NBS) which are mounted on instrument racks in the drywell. These transmitters sense the difference between the pressure due

to a constant reference leg of water and the pressure due to the actual height of water in the vessel. The four divisions of transmitters are shared with other systems within the respective divisions.

Drywell pressure is monitored by four pressure transmitters from the NBS which are mounted on instrument racks in the containment. These transmitters are also shared with other system channels within the respective divisions. The sensors provide inputs to local RDLCs which perform signal conditioning and analog-to-digital conversion. The formatted, digitized sensor inputs are transmitted with other sensor signals over an optical data link to the logic processing units in the main control room. The four signals from each parameter are combined, through appropriate optical isolators, in two-out-of-four logic for each division of the RHR/LPFL System. This assures that no single failure event can prevent initiation of the RHR/LPFL Systems. The initiation logic for the RHR System (including LPFL) is shown in Figure 7.3-4.

The LOCA signals (high drywell pressure and below reactor vessel water Level 1) which trigger the initiation logic also initiate starting of the respective division diesel generator.

The LPFL injection valve actuation logic requires a reactor low pressure permissive signal for automatic actuation on reactor water below Level 1 or high drywell pressure. The reactor pressure logic is a two-out-of-four network of shared sensor channels from the NBS and is similar in arrangement to the initiation logic just described.

Manual opening of the injection valve also requires the two-out-of-four reactor low pressure permissive.

(b) Logic and Sequencing

The overall LPFL operating sequence following the receipt of an initiation signal is as follows:

(i) The valves in the suction paths from the suppression pool are normally open and require no automatic action to line up suction.

(ii) Each of the three separate divisional RHR pumps will start, provided either normal or standby diesel power is available for the respective division.

(iii) Valves used in other RHR modes are automatically repositioned so that water pumped from the suppression pool is routed for LPFL operation.

(iv) When nuclear system pressure has dropped to within the proximity of the value at which the RHR System pumps are capable of injecting water into the vessel, the LPFL injection valves automatically open, and water

is delivered to the reactor vessel as the pressure continues to decay, until the vessel water level is adequate to provide core cooling. After adequate water level has been established, water flow may be diverted to containment or suppression pool cooling modes.

The transmitters which provide the initiation signals are from the NBS and are shared by other I&C system channels in common with each of the four divisions. This facilitates full two-out-of-four initiation logic for all LOCA parameters while utilizing efficient instrumentation. Optical isolators are used to provide proper separation of the electrical divisions. The four drywell pressure sensors supply isolated signals to the separate two-out-of-four logic of all three divisions of the RHR System. After an initiation signal is received by the LPFL control circuitry, the signal is sealed-in until manually reset. The logic is shown in Figure 7.3-4.

(c) Bypasses and Interlocks

The LPFL pump motor and injection valve are provided with manual override controls which permit the operator manual control of the system following automatic initiation. The RHR pumps are interlocked with corresponding bus undervoltage monitors. The pump motor circuit breakers will not close unless the voltage on the bus supplying the motors is above the setpoint of the undervoltage monitors.

(d) (LPFL) Redundancy and Diversity

The LPFL Subsystem is actuated by reactor vessel water below Level 1 and/or drywell high pressure. Either or both of these diverse conditions may result from a design basis LOCA and lesser LOCAs.

The RHR/LPFL System is completely redundant, in that three independent pump loops are provided, each having its own separate and independent AC and DC emergency power sources. Within the ECCS, the two divisions of HPCF and single division of RCIC also provide diverse and redundant methods for assuring adequate core cooling under postulated LOCA conditions.

(e) (LPFL) Actuated Devices

The functional control arrangement for the RHR/LPFL System pumps is shown in Figure 7.3-4. All three pumps start after a time delay, consistent with Table 6.3-1, provided normal or emergency power is available from their divisional sources. However, the diesel load sequence circuitry controls the demand placed on the onsite standby sources of power (Section 8.3). The delay times for the pumps to start when normal AC power is not available include approximately 3 seconds for the start signal to develop after the actual reactor

vessel water below Level 1 or drywell high pressure occurs, a time delay consistent with Table 6.3-1 for the standby power to become available, and a sequencing delay to reduce demand on standby power. The LPFL Subsystem is designed to provide flow into the reactor vessel within the time allowed by Table 6.3-1 of the receipt of the accident signals and the low reactor pressure permissive.

Two pressure transmitters and associated control room interfaces are installed in each pump discharge pipeline to verify that pumps are operating following an initiation signal. The pressure signals are used in the Automatic Depressurization Subsystem to verify availability of core cooling systems.

All automatic valves used in the LPFL function are equipped with remote-manual test capability. The entire system can be operated from the control room. Motor-operated valves have limit switches to turn off the motor when the full open or close positions are reached. Torque switches are also provided to control valve motor forces when valves are seating. Thermal overload devices are used to trip motor-operated valves during periodic tests and to provide alarms. Such overload devices are bypassed for safety events. Valves that have vessel and containment isolation requirements are discussed in Subsection 7.3.1.1.2.

The RHR System pump suction valve from the suppression pool is normally open. Shutdown cooling isolation valves must be closed to permit suction from the Suppression Pool. To reposition the valves, a keylock switch must be turned in the control room. On receipt of an LPFL initiation signal, the RHR test line valves are signaled to close (although they are normally closed) to ensure that the RHR System pump discharge is correctly routed.

The LOCA or manual initiation signal also sends a close signal to the normally closed heat exchanger bypass valves along with an open signal to the normally open heat exchanger outlet valves. This action assures proper orientation of these valves for the LOCA event.

(f) Separation

Separation of the RHR/LPFL I&C is in accordance with criteria stated in Subsection 8.3.1.4.2. LPFL circuits are unique to their assigned division except for the two-out-of-four initiation logics, which interface through optical isolators. All local cabling and equipment are located within divisionally assigned quadrants within the Reactor Building.

(g) Testability

The LPFL I&C equipment is capable of being tested during normal operation. Cross-channel comparison verifies analog transmitter outputs. Drywell pressure and low water level initiation transmitters can be individually valved out of service and subjected to a test pressure. This verifies the calibration range in addition to the operability of the transmitters. The instrument setpoint is verified by viewing the displays for each instrument. The logic is also tested as described in Subsection 7.1.2.1.6. Other control equipment is functionally tested during normal testing of each loop. Indications in the form of panel lamps and annunciators are provided in the control room.

All motor-operated valves and testable check valves (except injection valves and the shutdown valves) can be exercised and operationally tested during normal power operation. The injection valves and shutdown valves cannot be opened at normal reactor pressure.

(h) Environmental Considerations

The only control components pertinent to LPFL operation that are located inside the drywell are those controlling the gas-operated check valves on the injection lines. Other equipment located outside the drywell is selected in consideration of the normal and accident environments in which it must operate (Section 3.11).

(i) Operational Considerations

The pumps, valves, piping, etc., used for the LPFL are used for other operating modes of the RHR System. Initiation of the LPFL mode is automatic and no operator action is required for at least 30 minutes. Other RHR modes may be activated by Mode switches in the MCR. For example to enter the Containment Spray mode, this switch is first “Armed” and then the “Initiate” Push button is pressed. This assures that this is an intentional action by the operator. Also to transfer to these and other RHR Modes, mode specific permissives must be met. This reduces or eliminates the possibility of operator error.

Temperature, flow, pressure, and valve position indications are available in the control room for the operator to assess LPFL operation. Valves have indications for full-open and full-closed positions. Pumps have indications for pump running and pump stopped. Alarm and indication devices are shown in Figures 5.4-10 and 7.3-4.

(j) Parts of System Not Required for Safety

The non-safety-related portions of the LPFL Subsystem include the annunciators and the PCF. Other instrumentation considered non-safety-

related are those indicators which are provided for operator information, but are not essential to correct operator action.

7.3.1.1.2 Leak Detection and Isolation System (LDS)—Instrumentation and Controls

(1) System Identification

The instrumentation and control for the Leak Detection and Isolation System (LDS) consists of temperature, pressure, radiation and flow sensors with associated instrumentation and logic used to detect, indicate, and alarm leakage from the reactor primary pressure boundary. In certain cases, the LDS also initiates closure of isolation valves to shut off leakage external to the containment.

The MSIV function of LDS is implemented as part of the Reactor Trip and Isolation System (RTIS). All other LDS functions are implemented as part of ELCS.

Manual isolation control switches are provided to permit the operator to manually initiate (at the system level) isolation from the control room. In addition, each power-operated isolation valve is provided with a separate manual control switch in the control room which is independent of the automatic and manual leak detection isolation logic.

Paragraph (3), below, provides a description of the various input variables and sensing methods used to monitor the variables and provide the inputs to the LDS System for initiation of the isolation function. Each variable is recorded and/or indicated in the main control room.

(2) Supporting System (Power Sources)

LDS logic power is supplied by the respective divisional ELCS logic power supplies. See Section 8.3 for a description of the ELCS logic power supplies.

The power for the MSIVs pilot solenoid valve control logic is supplied from all four divisions of the RTIS buses. The MSIVs are spring-loaded, piston-operated pneumatic valves designed to fail closed on loss of electric power or pressure to the valve operator.

The motor-operated isolation shutdown cooling valves in the RHR shutdown cooling loop are isolated by power supplied from divisional power sources. RHR inboard valves are isolated by Division I logic for RHR A, by Division II logic for RHR B, and by Division III logic for RHR C. RHR outboard valves are isolated by Division II logic for RHR A, by Division III logic for RHR B, and by Division I logic for RHR C.

RCIC inboard valves are isolated by Division I logic. RCIC outboard valves are isolated by Division II logic.

(3) Input Variables and Sensing Methods

(a) RPV Low Water Level

Reactor vessel low water level signals are generated by differential pressure transmitters connected to taps located above and below the water level in the reactor vessel. The transmitters sense the difference between pressure caused by a constant reference leg of water and the pressure caused by the actual water level in the vessel. The ELCS monitors for low water level and provides trip signals in all four divisions at four different low reactor water levels. The signals are shared systems within the same division (i.e., RPS, ECCS) and are defined as follows:

(i) **Level 3—**This low level setting is the RPS low water scram setting. Level 3 is set high enough to indicate inadequate vessel water makeup possibly indicative of a breach in the reactor coolant pressure boundary (RCPB) or process piping containing reactor coolant, yet far enough below normal operation levels to avoid spurious isolation due to expected system transients. In addition to scram, trip of 40% of the Reactor Recirculation System (RRS) ten pumps and closure of the RHR shutdown cooling isolation valves are initiated at Level 3.

(ii) **Level 2—**The next lower setting (the setting for initiation of RCIC) is selected to avoid the release of radioactive material in excess of radiological limits outside the containment. The Level 2 setpoints are low enough so that the RCIC System will not be falsely initiated after a scram due to vessel low water level, provided feedwater flow has not been terminated. Conversely, the Level 2 setpoints are high enough so that for complete loss of feedwater flow, the RCIC System flow will be sufficient to avoid initiation of systems at Level 1-1/2. The remaining six RRS pumps are tripped and containment isolation valves (except drywell cooling isolation valves and MSIVs) are closed at Level 2. The RCIC System is shut down and/or isolated on high reactor water Level 8.

(iii) **Level 1-1/2—**The MSIVs are closed and the standby diesels and HPCF are started at Level 1-1/2. Level 1-1/2 shall be set low enough to prevent actuations of the above items on loss of feedwater pumps with reactor coolant makeup by the RCIC System. Level 1-1/2 shall be set high enough so that the HPCF System prevents a Level 1 actuation signal on loss of feedwater without RCIC operation.

(iv) **Level 1—**Automatic Depressurization Subsystem (ADS) operation is initiated at Level 1 (given a concurrent high drywell pressure signal or

following time out of the 8 minute drywell bypass timer) to enable the RHR System, when operating in the LPFL mode, to feed water into the reactor vessel. The RHR/LPFL mode is also initiated on Level 1.

ADS operation is initiated after low water Level (L1) for 8 minutes (ADS high drywell pressure bypass timer) and 29 seconds (ADS timer), plus makeup pumps running.

The reactor cooling water lines to the drywell air coolers are also isolated at Level 1.

Level 1 shall be set high enough to prevent excessive core heatup, assuming the most limiting pipe break (HPCF line break or main steamline break) and using licensing basis analytical assumptions.

Level indication is provided to show water level up to the top of the reactor vessel head. In addition, enhanced water level indication is provided to indicate water level from the core support plate to the nozzles of the main steamlines. All discrete levels are alarmed.

(b) Not Used

(c) Main Steamline Tunnel Area Temperature Monitors

Thermocouples are provided in the MSL tunnel area to monitor for high ambient temperature. The detectors are shielded so that they are sensitive to MSL area ambient temperature and not to radiated heat from hot equipment. The sensors provide input to the LDS for MSIV isolation when a preset high temperature condition (potentially indicative of a main steamline steam leak) is detected.

Also, the sensors provide a signal input to the CUW for isolation of its process lines.

(d) Main Steamline Flow Monitoring

Four differential pressure transmitters are used to monitor the flow in each MSL. The setting is selected high enough to permit closure of one MSIV for testing at rated power without causing isolation of the other MSLs, yet low enough to permit early detection of a steamline break. High steam flow in any two of the four MSLs will result in trip of the MSIV isolation logic to close the MSIVs and main steam drain valves. Valve isolation is annunciated in the control room.

(e) Main Steamline Low Pressure Monitoring

Four pressure transmitters are provided to sense the inlet pressure to the turbine and to initiate MSIV isolation on low pressure indications. These transmitters are located as close as possible to the turbine stop valves.

Steam pressure at the turbine inlet is monitored to provide protection against a rapid depressurization of the reactor vessel, which could be caused by the turbine bypass valves failing to the fully open position. The low pressure indication is annunciated in the control room.

(f) Main Condenser Low Vacuum Monitoring

Low main condenser vacuum could indicate that primary reactor coolant is being lost through the main condenser. Four divisional channels of the main condenser pressure monitoring are provided by the Nuclear Boiler System. The LDS utilizes the low vacuum signal to trip the MSIV isolation logic on low condenser vacuum, thereby closing the MSIVs and steamline drain valves. The condenser vacuum signal can be bypassed by a manual keylocked bypass switch in the control room during startup and shutdown operation.

(g) CUW Differential Flow Monitoring

The suction and discharge flows of the Reactor Water Cleanup System (CUW) are monitored for flow differences. Flow differences greater than preset values cause alarm and isolation. Delay timers provide for delaying the isolation signal to accommodate normal system surge conditions. Four divisional channels of flow measurements are provided by the LDS on each process line for this function as follows: flow in the CUW suction line from the reactor, flow in the CUW return lines to the reactor, and flow in the blowdown line to the main condenser are monitored. The temperature-compensated flow output in the suction line is compared with the flow outputs from the discharge lines by electronic equipment which trips on high differential flow. The Division II channel trip will close the inboard CUW isolation valves and Division I channel trip will close the CUW outboard isolation valves.

(h) Drywell Pressure Monitoring

Drywell pressure is monitored by four divisional pressure transmitters relative to containment pressure. These transmitters are provided by the Nuclear Boiler System and are shared with other systems. The transmitters are mounted in local panels within the Reactor Building. Instrument sensing lines that connect the transmitters with the drywell interior physically interface with the containment system.

Four channels (one in each of the four divisions) provide signals to LDS isolation logic.

(i) Drywell Air Cooler Condensate Flow Monitoring

The condensate flow rates from the drywell atmosphere coolers are monitored for high drain flow, which indicate leaks from piping or equipment within the drywell. This flow is monitored by one channel of flow instrumentation located to measure flow in the common condensate cooler drain line which drains the condensate from all of the drywell coolers to the drywell floor drain sump. The high flow indication is alarmed in the control room.

(j) RCIC Steamline Flow Monitoring

The steam supply line which provides motive power to drive the RCIC turbine is monitored for abnormal flow. Four channels of flow measurements are provided by the LDS for detection of steamline breaks by flow transmitters which sense differential pressure across elbow taps in the steamline. A trip signal from Division II isolation logic will close the outboard isolation valve, while a Division I trip will close the inboard RCIC steamline isolation valve and the warmup bypass valve. Any isolation signal to the RCIC logic will also trip the RCIC turbine. The elbows and taps are shown on the RCIC P&ID (Figure 5.4-8). The transmitters and associated trip channels are shown on the LDS IED (Figure 5.2-8).

(k) Drywell Temperature Monitoring

The ambient temperature within the drywell is monitored by four thermocouples located equally spaced in the vertical direction within the drywell. An abnormal increase in drywell temperature could indicate a leak within the drywell. Ambient temperatures within the drywell are recorded and alarmed in the control room.

(l) Valve Leakage Monitoring

Safety/relief valve(SRV) leakage is monitored by temperature sensors located on each relief valve discharge line. The monitoring of this leakage is provided by the Nuclear Boiler System.

(m) Drywell and Secondary Containment Sump Monitoring

Each sump monitoring system is equipped with two pumps and control instrumentation. The two drywell drain sumps are each equipped with a sonic level element and a level transmitter for monitoring level changes in the sump. The instrumentation provides indication and alarm of excessive fill rate or pumpout frequency of the sumps. The rate at which the drain sump fills with

reference to the frequency of sump pump operation determines the leakage rate. The drain sump instrumentation has a sensitivity of detecting reactor coolant leakage of 3.785 L/min within a 60-minute period. Alarm setpoints (nominal values) established at 114 L/min for floor and equipment drain sumps (total leakage) to 19 L/min for floor drain sumps and 8 L/min for increase floor drain sump flow within the previous 4 hours. The drywell floor drain sump collects unidentified leakage from such sources as floor drains, valve flanges, closed cooling water for reactor services and condensate from the drywell atmosphere coolers. The drywell equipment drain sump collects identified leakage from known sources.

(n) Inter-System Radiation Leakage Monitoring

Radiation monitors are used to detect reactor coolant leakage into Reactor Building Cooling Water (RCW) systems supplying the RHR heat exchangers and the CUW heat exchangers. These monitoring channels are part of the Process Radiation Monitoring System (Section 7.6). One radiation monitoring channel is provided to monitor for reactor coolant leakage into each RCW loop downstream of the RHR heat exchangers and the CUW nonregenerative heat exchangers. Each channel will alarm on high radiation, indicating process leakage into the cooling water. No isolation trip functions are performed by this monitor.

(o) Drywell Fission Product Monitoring

Primary coolant leaks within the drywell are detected by radiation monitoring of drywell atmosphere samples. The fission product radiation monitor provides gross counting of radiation from radioactive particulates, iodine, and noble gases. The count levels are recorded in the control room and alarmed on abnormally high activity level of any of the three variables. The fission product monitoring subsystem and its sampling arrangement are shown on the LDS IED (Figure 5.2-8).

(p) Temperature Monitors in Equipment Areas

Thermocouple temperature elements are installed in the RCIC, RHR, and CUW equipment rooms for sensing high ambient temperature in the areas. These elements are located or shielded so that they are sensitive to air temperature only and not to radiated heat from hot equipment. The high temperature trip is alarmed in the control room for each area and is used for isolation of the affected system process lines.

(q) RCIC Steamline Pressure Monitors

Pressure in the RCIC steamline is monitored to provide RCIC turbine shutoff and closure of the RCIC isolation valves on low steamline pressure as a protection for the turbine. This line pressure is monitored by pressure transmitters connected to one tap of the elbows used for flow measurement upstream of the steamline isolation valves (see Paragraph j). Four divisional channels of monitoring are provided for RCIC isolation. Division 1 isolation signal isolates the inboard valves, while Division 2 isolation signal isolates the outboard valves.

(r) RCIC Turbine Exhaust Line Pressure Monitors

Pressure in the RCIC System turbine exhaust vent line is monitored by four channels of pressure instrumentation (two in Division I and two in Division II). Both logic channels of Division I trip on high turbine exhaust pressure to close the inboard RCIC isolation valves and trip the turbine. Both logic channels of Division II trip to close the outboard RCIC isolation valve and trip the turbine. The instrumentation channel equipment and piping are provided by the RCIC System as an interface to the LDS.

(s) Reactor Vessel Head Flange Seal Leakage Monitoring

A single channel of pressure monitoring is provided for measurement of pressure between the inner and outer reactor head flange seals. High pressure will indicate a leak in the inner seal. This pressure is monitored by the Nuclear Boiler System and is annunciated in the control room (no isolation). Leakage through both inner and outer seals is routed to the drywell equipment drain sump.

(t) Reactor Recirculation Pump Motor Leakage Monitoring

Excess leakage of the motor casing will be detected by the drywell floor drain sump monitors described in Paragraph (m).

(u) Containment Isolation Signals

The following signals and controls are provided for containment isolation.

(i) Four division channels of high drywell pressure signals

(ii) Four divisional signals for each low reactor vessel water Level 1, 1.5, 2, and 3 signals

(iii) Division I, II, and III manual isolation controls

(iv) Manual logic reset controls

(v) Trip signals from the Process Radiation Monitor System are provided for isolation of the secondary containment

(v) Main Steamline Temperature Monitoring in Turbine Building

The LDS monitors the ambient temperatures along the main steamline in the turbine building for main steamline leakage. Output signals from four monitoring divisional channels are used for inputs to MSIV isolation logic.

(w) Feedwater Line Differential Pressure

The LDS monitors the differential pressure to detect a break in the piping. If a confirmatory high drywell pressure signal is also present then a trip of the condensate pumps is initiated.

(4) Signal Initiating Signals

The trip signals listed above provide inputs to the automatic isolation logic for closure of the valves in the various pipelines and systems as delineated in Table 5.2-6.

For a detailed description of all containment penetrations and isolation valves closed for the above systems, see Section 6.2.

(5) System Sequencing and Logic

(a) Main Steamline Isolation

For main steamline isolation, each variable is independently monitored by one instrument channel in each of the four divisions. Each instrument channel, in turn, provides an input to all four divisions (with appropriate signal isolation) of two-out-of-four logics. Each two-out-of-four logic provides inputs to one of the four separate divisional trip logics.

Each MSIV is controlled by redundant solenoids (powered by different electrical divisions) on each valve. Two solenoids on a given valve must be simultaneously de-energized to close the valve. All four electrical power divisions are utilized in the control logic such that two-out-of-four failsafe logic is employed to de-energize both solenoids and thus achieve isolation (Figure 7.3-5). The outboard main steamline drain valve closes if either Division I or Division IV logic channel trips. The inboard main steamline drain valves close if either Division II or Division III logic channel trips.

(b) Other Process Line Isolation

All systems are isolated by fail-safe “de-energize to isolate” logic.

RHR inboard valves are isolated by Division I logic for RHR A, by Division II logic for RHR B, and by Division III logic for RHR C.

RHR outboard valves are isolated by Division II logic for RHR A, by Division III logic for RHR B, and by Division I logic for RHR C.

The RCIC inboard valve is isolated by Division I logic. The RCIC outboard valve is isolated by Division II logic.

After reactor water below Level 1 or high drywell pressure, LDS provides the ATIP System with an isolation signal to initiate TIP withdrawal followed by closure of the ball valves and purge line valves.

The response time of the instrument channels and control logic for automatic isolation initiation is compatible with the closure time requirements of individual system isolation valves.

The LDS logic also provides for manual initiation or isolation of all automatic isolation valves. Additionally, all system isolation valves have individual manual control switches and position indication located on their individual system control panels. However, the LDS isolation logic will override the individual manual controls to close all system isolation valves regardless of manual control switch position.

Direct operator action is required (via a logic reset) to manually reset the trip condition. (The initiating signal must be cleared before the logic can be reset.) The isolation valve cannot be reopened until the trip logic is reset. For detailed logic, see Figure 7.3-5.

(6) LDS Bypasses and Interlocks

Each of the four safety-related logic divisions is provided with a separate keylocked bypass switch which will bypass all instrument channel inputs to the two-out-of-four logics in its respective division. These four divisional bypass switches are provided in the control room and are interlocked such that only one divisional bypass can be implemented at a time. With a bypass actuated, the two-out-of-four logic is effectively converted to a two-out-of-three logic. These same four bypass switches are used to bypass the Reactor Protection System instrument channels. The MSL turbine inlet pressure channels are bypassed by the reactor mode switch in all reactor modes except in the RUN mode. This is an operational bypass. The main condenser

low vacuum channels are provided with a keylocked operational bypass for use during plant startup. This bypass is provided in the control room.

Also, bypass of the main condenser vacuum channels is provided when the reactor dome pressure is low or when the turbine stop valve is less than 90% open. These are considered system interlocks.

(7) Redundancy and Diversity

(a) Main Steamline

Redundancy is provided by the instrumentation to monitor each essential variable as follows:

(i) Four divisional reactor water level channels monitor for low reactor vessel level (L1.5).

(ii) Four divisional differential pressure channels monitor for high MSL flow for each MSL.

(iii) Not Used

(iv) Four divisional temperature instrument channels monitor for high ambient temperature in the MSL tunnel.

(v) Four divisional temperature instrument channels monitor for high MSL area temperature in the Turbine Building along the MSL to the turbine.

(vi) Four divisional pressure transmitters monitor for low main condenser vacuum.

(vii) Four divisional pressure transmitters monitor for low MSL pressure at the inlet to the main turbine.

The above instrumented channels provide diversity in monitoring for a leakage outside the containment.

(b) Reactor Water Cleanup

Redundancy is provided by instruments monitoring each essential variable as follows:

(i) Four main steamline tunnel area temperature channels

(ii) Four differential mass flow divisional channels

(iii) Four divisional ambient temperature channels located in each CUW equipment hot area

(iv) Four reactor vessel water level (L2) channels shared with other ESF systems

Diversity for detecting CUW line break is provided by instrumentation for differential flow and equipment area ambient temperature monitoring channels.

(c) Residual Heat Removal/Shutdown Cooling Suction Lines

Redundancy is provided by instruments monitoring each essential variable as follows:

(i) Four reactor pressure monitoring channels shared with other ESF systems (one in each of four divisions) to provide low reactor pressure permissive.

(ii) Four reactor vessel low water level monitoring channels shared with other ESF systems (one in each of four divisions) to provide isolation on Level 3.

(iii) Four divisional ambient temperature channels are provided (one set per RHR loop) in each RHR equipment area.

(d) Reactor Core Isolation Cooling (RCIC)

Redundant divisional instrument channels are provided to monitor essential system variables for RCIC isolation:

(i) Four divisional RCIC equipment area ambient temperature monitoring channels (one in each division)

(ii) Four RCIC turbine exhaust pressure monitoring channels (two in each of two divisions)

(iii) Four divisional RCIC steamline pressure monitoring channels (one in each division)

(iv) Four divisional RCIC steam line flow monitoring channels (one in each division)

(e) Manual Control

Redundancy and freedom from spurious manual initiation is provided by four selector pushbuttons (one in each of four divisions) for manual system level main steamline isolation. The isolation circuits for RHR, CUW, RCIC, etc., likewise have manual initiation switches for each division of the system(s).

Diversity is provided for manual isolation by system level manual isolation switches and independent valve control switches.

(f) Redundancy of logic is discussed in Subsection 7.3.1.1.2 (5).

(g) Redundancy of isolation valves is discussed in Subsection 6.2.4.

(h) Redundancy of logic power divisions is discussed in Subsection 7.3.1.1.2(2).

(8) Actuated Devices

(a) The main steamline isolation valves are spring and pneumatic closing, piston-operated valves (Figure 5.4-7). They close by spring power on loss of pneumatic pressure to the valve operator. This is a fail-safe design.

The control arrangement is shown in the LDS/IBD (Figure 7.3-5). Closure time for the valves is set between 3 and 5 seconds. Each valve is controlled by three-way solenoid-operated pilot valves, powered by 120 VAC. Position limit switches are provided for logic interfaces and valve position indication.

(b) Motor-operated isolation valves are controlled by motor control centers with initiating control from the control room logics. The motor operators for all valves, except throttling valves, are provided with seal-in circuits to ensure complete valve travel once initiated. All motor-operated valves are provided with close direction torque switches to ensure tight closure. Limit switches are provided for valve interlocks and valve position indication.

(c) Direct solenoid-operated valves are energized to open and close by spring force for isolation. Valves are controlled from the control room and provided with valve position indicators.

(d) The solenoid-operated pneumatic valves are normally energized to open, and will fail-closed. In the event of power or pneumatic supply failure, the valves will automatically close. The closure times of the valves are based on system requirements. The isolation valves are provided with open/close position switches to provide for control room indications.

(e) All power-operated valves incorporate limit and torque switches for control and for position indication in the control room.

(9) Separation

Electrical and mechanical separation complies with the criteria presented in Subsection 8.3.1.4.2.

(10) Testability

Pressure or differential pressure type sensors, used for monitoring level, pressure, or flow, may be valved out of service one at a time and functionally tested using a test pressure source. A remotely actuated check-source is provided with each detector or group of detectors for test purposes.

(11) Environmental Considerations

The physical and electrical arrangement of the LDS was selected so that no single physical event would prevent achievement of isolation functions. Motor operators for valves inside the drywell are of the totally enclosed type; those outside the containment have weather-proof enclosures. Solenoid valves used as air pilots are provided with watertight enclosures. All cables and operators are capable of operation in the most unfavorable ambient conditions anticipated for normal operations. Temperature, pressure, humidity, and radiation are considered in the selection of all equipment, including sensors and control room equipment, for the system. Cables used in high radiation areas have radiation-resistant insulation. Shielded cables are used where necessary to eliminate interference from magnetic fields.

Special consideration has been given to isolation requirements during a loss-of-coolant accident inside the drywell. Components of the LDS that are located inside the drywell and that must operate during a LOCA are the cables, control mechanisms and valve operators of isolation valves inside the drywell. These isolation components are required to be functional in a LOCA environment (Section 3.11). Electrical cables are selected with insulation designed for this service. Closing mechanisms and valve operators are considered satisfactory for use in the isolation control system only after completion of environmental testing under LOCA conditions or submittal of evidence from the manufacturer describing the results of suitable prior tests.

(12) Operational Considerations

The LDS is on continuously to monitor containment leakage during normal plant operation. The system will automatically function to isolate a reactor coolant leak external to the containment and prevent unacceptable radiological releases from the containment following detection of a leakage within the containment. No operator action is required following system initiation.

The following information is alarmed and/or indicated in the control room. Indication is provided by instruments, displays, recorders, status lights, computer readout or annunciator alarms:

— Manual system level isolation

— Instrument channel trips

— Isolation logic trips (initiation of isolation)

— Logic failures or out of service

— All bypasses

— Valve overrides

— Test status

— Power supply failures

— Individual valve position indication adjacent to valve control switches

All non-essential indications and alarms (i.e., annunciator, computer inputs) are electrically and physically isolated from the isolation logics to preserve the integrity of the isolation function in the event of a failure in non-safety-related equipment.

The CUW isolation logic receives inputs originating from starting the Standby Liquid Control (SLC) System. These input signals are required to isolate the CUW when the SLC System is started. The RHR System isolation logic is provided with input signals from pressure transmitters monitoring reactor pressure. These pressure transmitters prevent opening the RHR shutdown cooling valves and CUW head spray valve whenever the reactor pressure is above a preset value. This signal is provided as an interlock and is not provided for containment or reactor vessel isolation.

(13) Parts of System Not Required for Safety

The non-safety-related portions of the LDS include the circuits that drive annunciators and the PCF. Other instrumentation considered non-safety-related are those indicators which are provided for operator information.

7.3.1.1.3 RHR/Wetwell and Drywell Spray Cooling Mode—Instrumentation and Controls

(1) System Identification

Wetwell/drywell spray cooling (WDSC) is a manually-initiated operating mode of the RHR System (see Figure 5.4-10 P&ID). It is designed to provide the capability of condensing steam in the wetwell air volume and the containment atmosphere and removing heat from the suppression pool water volume.

(2) Supporting Systems (Power Sources)

Power for the RHR System pumps B and C is supplied from two independent AC buses that can receive standby AC power. Motive and control power for the two divisions of WDSC and I&C equipment are the same as those used for LPFL B and C, respectively (Subsection 7.3.1.1.4).

(3) Equipment Design

Control and instrumentation for the following equipment is required for this mode of operation:

(a) Two RHR main system pumps

(b) Pump suction valves

(c) Drywell spray discharge valves

(d) Wetwell spray discharge valves

Variables needed for the operation of the drywell spray equipment are high pressure conditions in the drywell air space. The instrumentation for wetwell and drywell spray operation ensures that water will be routed from the suppression pool to the wetwell and drywell air volumes.

Wetwell and drywell spray operation uses two pump loops, each loop with its own separate discharge valve. All components pertinent to wetwell and drywell spray operation are located outside of the drywell.

Motive and control power for the two loops of wetwell and drywell spray I&C equipment are the same as those used for RHR B and RHR C.

The drywell spray cooling mode can be manually initiated from the control room if the RHR injection valve is fully closed and the drywell pressure is above a setpoint, allowing the operator to act in the event of a LOCA. In the absence of high drywell pressure conditions, the drywell spray valves cannot be opened.

The wetwell spray cooling can be manually initiated in the control room. The operator relies on the instrumentation that provides indication of the wetwell air space temperature condition when initiating this mode. No interlock is provided.

(a) Initiating Circuits

Drywell Spray B: Drywell pressure is monitored by four shared pressure transmitters mounted in instrument racks in the containment.

Signals from these transmitters are routed to the local RDLCs which convert analog to digital signals and send them through fiber optic links for logic processing in the control room. Any two-out-of-four signals provide the permissive to manually initiate the Drywell Spray Mode.

Initiation logic for drywell spray B is identical to drywell spray C.

Wetwell Spray B: The initiation of wetwell spray mode is manual and can be initiated provided RPV Water Level is above Level 1. The operator bases judgment on the instrumentation indication of the condition of the wetwell air space temperature.

Operation of wetwell spray B is identical to wetwell spray C.

(b) Logic Sequencing

Wetwell and or Drywell Spray Modes can be entered separately or by initiating the Containment Spray Mode (which activates both). Most commonly this occurs after LPFL initiation.

The operating sequence once either the Containment Spray Mode, Wetwell Spray Mode, or Drywell Spray Mode is selected after LPFL initiation is as follows:

(i) The RHR pumps continue operating.

(ii) Valves in other RHR modes are automatically repositioned to the Wetwell / Drywell Spray Modes.

(iii) The service water pumps continue running.

(iv) Service water supply and discharge valves to the RHR heat exchanger remain open.

(v) The heat exchanger outlet valve opens and the heat exchanger bypass valve is signaled to close.

(vi) Vessel injection is terminated when the RHR Containment Spray Mode is selected. Alternately the Drywell or Wetwell spray modes can be initiated independently.

(vii) In the presence of high drywell pressure, the Drywell spray valves will automatically open.

(viii) The wetwell spray valve will open to perform the spray function without any permissives.

The spray system will continue to operate until manually terminated by the operator or will automatically terminate and realign to the LPFL injection mode on receipt of a reactor vessel water below Level 1, since core cooling has priority.

(c) Bypass and Interlocks

No bypasses are provided for the wetwell and drywell spray system.

The RHR pumps are interlocked with corresponding bus undervoltage monitors. The pump motor circuit breakers will not close unless the voltage on

the bus supplying the motors is above the setpoint of the undervoltage monitors.

A high drywell pressure signal is provided as a permissive for opening the drywell spray valves. In addition, the spray valves are prevented from opening unless the RHR injection valve is fully closed.

The wetwell spray function is interlocked with reactor vessel water Level 1 as described in 7.3.1.1.3(a).

(d) Redundancy and Diversity

Redundancy is provided for the wetwell and drywell spray function by two separated divisional loops. Redundancy of initiating sensors is described in Subsection 7.3.1.1.4.

(e) Actuated Devices

Figure 7.3-4 shows functional control arrangement of the Wetwell and Drywell Spray System.

The RHR B and C loops are utilized for wetwell and drywell spray. Therefore, the pumps and valves are the same for the LPFL and wetwell and drywell spray except that each has its own discharge valve. See Subsection 7.3.1.1.4 (LPFL Actuated Devices) for specific information.

(f) Separation

Separation of the WDCS RHR is in accordance with criteria stated in Subsection 8.3.1.4.2.

Wetwell and drywell spray is a Division II (RHR B) and Division III (RHR C) system. Manual controls, logic circuits, cabling, and instrumentation for containment spray are arranged such that divisional separation is maintained.

(g) Testability

The Wetwell and Drywell Spray System is capable of being tested up to the last discharge valve during normal operation. Drywell and wetwell pressure channels are tested by cross-comparison between related channels. Any disagreement between the display readings for the channels would indicate a failure. The instrument setpoint is verified by viewing the displays for each instrument. Testing for functional operability of the control logics is accomplished as described in Subsection 7.1.2.1.6. Other control equipment is functionally tested during manual testing of each loop. Indications in the form of panel lamps and annunciators are provided in the control room.

(h) Environmental Considerations

Refer to Section 3.11 for environmental qualifications of the subject system equipment.

(i) Operational Considerations

Wetwell and drywell spray is a mode of the RHR System, and is not required during normal operation.

Temperature, flow, pressure, and valve position indications are available in the control room for the operator to assess wetwell and drywell spray operation (except for the wetwell spray which does not have pressure). Alarms and indications are shown in Figures 5.4-10 (RHR P&ID) and 7.3-4 (RHR IBD).

Chapter 16 describes the methods for calculating setpoints and margins.

(j) Parts of System Not Required for Safety

The non-safety-related portions of the WDCS-RHR include the annunciators and the PCF. Other instrumentation considered non-safety-related are those indicators which are provided for operator information, but are not essential to correct operator action.

7.3.1.1.4 RHR/Suppression Pool Cooling Mode—Instrumentation and Control

(1) System Identification

Suppression pool cooling is an operating mode of the RHR System. It is designed to provide the capability of removing heat from the suppression pool water volume. The system is automatically initiated upon receipt of a high temperature signal from the suppression pool temperature monitoring system (SPTM) or may be manually initiated when necessary.

(2) Supporting Systems (Power Sources)

Power for RHR System pumps A, B, and C is supplied from three independent AC buses that can receive standby AC power. Motive and control power for the three loops of suppression pool cooling instrumentation and control equipment are the same as that used for LPFL A, B, and C, respectively.

(3) Equipment Design

Control and instrumentation for the following equipment is required for this mode of operation:

— Three RHR main system pumps

— Pump suction valves

— Suppression pool discharge valves

Suppression Pool Cooling (SPC) uses three pump loops, each loop with its own separate discharge valve. All I&C components pertinent to suppression pool cooling operation, except suppression pool temperature monitoring, are located outside of the drywell.

The Suppression Pool Cooling (SPC) mode is automatically initiated on high suppression pool temperature or manually initiated from the control room. This mode is put into operation to limit the water temperature in the suppression pool such that the temperature immediately after a blowdown does not exceed the established limit when reactor pressure is above the limit for cold shutdown.

(a) Initiating Circuits

Initiating suppression pool cooling is automatic upon receipt of high suppression pool temperature signals from the SPTM system. SP cooling may also be initiated manually by the control room operator during normal operation, abnormal transients, or post LOCA events. Initiation of suppression pool cooling A is identical to that of B and C.

(b) Logic and Sequencing

The operating sequence of suppression pool cooling, following indication that SP temperature is HIGH, is as follows:

(i) The RHR System pumps are started or continue to operate.

(ii) Valves in other RHR modes are automatically repositioned to align to SPC mode.

(iii) RHR service water discharge valves to the RHR heat exchanger are opened.

(iv) If performed following LPFL initiation, the Suppression Pool Cooling Modes switch is first “Armed” and the “Initiate” pushbutton is pushed. At that time the injection valves are manually closed and SP valves are opened.

(v) The SPC mode will continue to operate until the operator activates another permitted mode or when reactor water below Level 1 reoccurs, in which case the injection valve will auto-open and the SP discharge valve will auto-close.

(vi) Automatic initiation of the SPC mode can only happen when initiated from the RHR Standby Mode. The operator must terminate this mode manually.

(c) Bypasses and Interlocks

The SPC mode does not have interlocks and can be operated anytime except during a LOCA, where the cooling mode (LPFL) has priority. For manual operation, the operator relies on instrumentation that provides the temperature condition of the suppression pool in the control room.

The RHR pumps are interlocked with corresponding bus undervoltage monitors.

The pump motor circuit breakers will not close unless the voltage on the bus supplying the motors is above the setpoint of the undervoltage monitors.

(d) Redundancy and Diversity

Redundancy is provided for the SPC function by three separate divisional logics, one for each loop.

(e) Actuated Devices

Figure 7.3-4 shows the interlock block diagram of the SPC mode.

The RHR A, B, and C loops are utilized for SPC. Therefore, the pump and valves are the same for LPFL and SPC, except that each mode has its own discharge valves.

(f) Separation

Separation of the SPC-RHR is in accordance with criteria stated in Subsection 8.3.3.6.2.

Suppression pool cooling is a Division I (RHR A), Division II (RHR B) and Division III (RHR C) system. Automatic and manual control, logic circuits, and instrumentation for suppression pool cooling are arranged such that divisional separation is maintained.

(g) Testability

Suppression pool cooling is capable of being tested during normal operation.

Testing for functional operability of the control logic can be accomplished as described in Subsection 7.1.2.1.6.

Indications in the form of panel indicators and annunciators are provided in the control room.

(h) Environmental Considerations

Refer to Section 3.11 for environmental qualifications of the system components.

(i) Operational Considerations

Suppression pool cooling is a mode of the RHR System and can be used during normal power operation to limit suppression pool temperature. Temperature, flow, pressure, and valve position indications are available in the control room for the operator to assess SPC operation. Alarms and indications are shown in Figure 7.3-4.

Alarm setpoints for high suppression pool (SP) temperatures are provided in the SP temperature monitoring system. The SP cooling system is manually or automatically initiated if a persistent increase of SP temperature occurs.

(j) Parts of System Not Required for Safety

The non-safety-related portions of the SPC-RHR include the annunciators and the PCF. Other instrumentation considered non-safety-related are those indicators which are provided for operator information, but are not essential to correct operator action.

7.3.1.1.5 Standby Gas Treatment System—Instrumentation and Controls

(1) System Identification

The Standby Gas Treatment System (SGTS) processes gaseous effluent from the primary and secondary containments when required to limit the discharge of radioactivity to the environment during normal and abnormal operation. It also controls the exfiltration of fission products by maintaining a negative pressure in the secondary containment, and by filtering the effluent prior to discharge to the atmosphere following a LOCA or fuel handling accident. System drawings are given in Figures 6.5-1 and 7.3-6.

(2) Supporting Systems (Power Sources)

The instrumentation and controls of the SGTS are supplied by the emergency power supply system (Division II and Division III).

(3) Equipment Design

Process gas flow is controlled manually by a motor-driven butterfly valve located on the upstream of the filter train.

The relative humidity of the air entering the charcoal adsorber is sensed by a humidity element downstream of the electric space heaters. A controller operates the space heaters to maintain the relative humidity of the air at 70% or less. The switch initiates an alarm in the control room upon high air temperature.

Temperature sensors determine the charcoal bed temperature. A switch actuates a control room annunciator upon high and high-high temperature in the charcoal.

(a) Initiating Circuits

The SGTS is initiated automatically upon detection of a LOCA (high drywell pressure or low reactor water level), or by high radiation in the fuel handling area or secondary containment HVAC exhaust air. It can also be initiated manually from the main control room.

Upon initiation of the SGTS, both redundant trains start operating initially. Subsequently, one train may be manually shut down and placed on standby, but may be reinitiated by low airflow in the operating filter train.

Upon receiving a high charcoal temperature signal, the cooling fans are manually started. The operator may stop the fan if the charcoal temperature is below the setpoint and is not rising.

(b) Logic and Sequencing

Initiation of the SGTS also deenergizes the pressure control supply and the exhaust fans of the secondary containment. The secondary containment isolation dampers will close.

(c) Bypasses and Interlocks

Interlocks for SGTS valves and heaters assure their operation when the fans are running.

Differential pressure indicators show the pressure drop across the prefilters and the HEPA filters. Transmitters upstream of the filter train monitor SGTS flow. If flow decreases below a preset limit, an annunciator is actuated in the main control room.

(d) Redundancy and Diversity

Two independent and redundant filter trains are provided, including independent and redundant logic and mechanical equipment. The two logic systems and their associated mechanical devices are powered from separate ESF buses. These trains contain active components, such as fans and heaters. Physical and electrical separation is maintained between the two filter trains.

(e) Actuated Devices

Control devices actuated by the SGTS are shown on the interconnection block diagram, Figure 7.3-6.

(f) Separation

The control and logic circuits of the filter trains are physically and electrically separated to reduce the probability that a single physical event may prevent operation of the SGTS. Electric cables for redundant instrumentation and controls on the two divisions of the SGTS are routed separately.

(g) Testability

Control and logic circuitry used in the controls for the active components of the SGTS can be individually checked by applying test or calibration signals to the sensors and observing trip or control responses. Operation of dampers and fans from manual switches verifies the ability of damper mechanisms to operate. The automatic control circuitry is designed to initiate SGTS operation if a fuel-handling accident or LOCA occurs during a test.

(h) Environmental Considerations

Temperature, pressure, humidity, and radiation are considered in the selection of equipment for the SGTS instrumentation and controls.

For the environment in which the SGTS instrumentation and control components are located, refer to Section 3.11.

(i) Operational Considerations

The SGTS fans can be started and dampers opened or closed on a system level or individual basis by manipulating switches in the main control room, thus providing the operator with means independent of the automatic initiation functions.

The SGTS is designed so that, once initiated, the dampers continue to operate to the end of their strokes and the fans continue to run, even if the condition that caused initiation is restored to normal.

The operator must manually operate switches in the main control room to shut down a standby gas treatment unit which has been automatically started.

Initiation of the SGTS is annunciated in the main control room so that the operator is immediately informed of the condition. The status of fans and dampers is indicated by lights on the control panel.

The SGTS is designed to start both filter trains automatically and simultaneously. When both units are operating, the operator may place one of the two trains on standby. Should the operating unit fail, the standby unit can be automatically initiated.

(j) Parts of System Not Required for Safety

The non-safety-related portions of the SGTS include the annunciators and the PCF. Other instrumentation considered non-safety-related are those indicators which are provided for operator information, but are not essential to correct operator action.

7.3.1.1.6 Emergency Diesel Generator Support Systems

Division I, II, and III diesel generator system control and instrumentation is discussed in Subsection 8.3.1.1.8.

The diesel generator auxiliary systems are described in subsections of Chapter 9 and are listed below:

(a) Diesel generator jacket water system

(b) Diesel generator starting air system

(c) Diesel generator lubrication system

(d) Diesel fuel storage and transfer system

(e) Diesel combustion air intake and exhaust system

7.3.1.1.7 Reactor Building Cooling Water System and Reactor Service Water System—Instrumentation and Controls

(1) System Identification

The control system for the Reactor Building Cooling Water (RCW) System and Reactor Service Water System operates to maintain the flow of cooling water to operate auxiliaries which are required for normal plant operation and normal or emergency reactor shutdown, as well as to those auxiliaries whose operation is desired following a LOCA but not essential to safe shutdown.

The RCW/RSW System is comprised of three divisions as shown in Figure 9.2-1. Control system details for both RCW and RSW Systems are shown in the interlocking block diagram (Figure 7.3-7). The RSW System is also comprised of three divisions as shown in Figure 9.2-7.

(2) Power Sources

The power for RCW System instrumentation and controls is supplied from Division I, II, and III 125 VDC and 120 VAC essential power buses.

(3) Equipment Design

During normal operation, RCW water flows through the safety-related and non-safety-related equipment except the RHR and emergency diesel jacket water cooling heat exchangers.

During all plant operating modes, one RCW pump is normally operating in each division, so that in the event of LOCA, the RCW Systems required to shut down the plant safely are already in operation.

Isolation of the non-safety-related section of each division of the RCW System from the safety-related section is accomplished by motor operated valves in the inlet and outlet lines to the non-safety-related section. Flow sensors are located in the inlet lines.

(a) Initiating Circuits

During normal operation, all RCW and RSW divisions supply both safety-related and non-safety-related cooling loads. Except for instrument air, FPC fuel pool, FPC room, service air, CUW pump, and CRD oil cooling, the non-safety-related loads are automatically isolated upon a LOCA. All non-safety-related loads except for FPC fuel pool and FPC room cooling are isolated on occurrence of RCW surge tank low level (two-out-of-three logic). Isolation can also be initiated manually from the control room.

All of the safety-related portions of the RCW System are started automatically (standby pumps start and standby valves open) upon a LOCA and/or LOPP (as defined in Subsection 8.3.1.1.7). The containment isolation valves are closed automatically upon receipt of the LOCA signal or may be closed manually from the control room.

(b) Logic and Sequencing

The LOCA signal used to actuate the RCW water isolation system is derived from the two-out-of-four logic of reactor low level or high drywell pressure trip signals. The signal is generated by either:

(i) Two-of-four level sensors being tripped.

(ii) Two-of-four pressure sensors being tripped.

(iii) Both sets of the above.

Once an initiation signal is received, the signal is sealed in until manually reset.

The isolation valves stay closed until the LOCA signal is no longer present or a control switch is operated in the control room.

(c) Bypass and Interlocks

The LOCA signal that automatically initiates the non-safety-related service water isolation system can be overridden by a control switch in the control room. If the operator determines that the non-safety-related auxiliaries are operable, flow can be initiated by a combination LOCA override and manual valve-opening operation. The remote shutdown panel has control transfer capability to take manual control of Divisions I and II of the RCW System. (See Subsection 7.4.1.4.4(5) for RSS interface.)

(d) Redundancy and Diversity

The RCW and RSW System instrumentation and power supplies are separated into three divisions such that no single occurrence results in the loss of function of more than one division. Overall redundancy is provided by separated, divisional service water loops for Divisions I, II, and III.

(e) Actuated Devices

The automatically actuated isolation valves in the RCW and RSW System are provided with electric motor operators. The valve limit switches turn off the motor when the valves are fully open and permit torque switches to control valve motor forces while the valves are seating in the closed direction. Other valves have torque limits in the open direction except at breakaway and torque limits on closing.

(f) Separation

RSW System trip channels, logic circuits, manual controls, cabling and instruments are mounted so that Division I, II, and III separation is maintained in accordance with Subsection 8.3.3.1 criteria.

(g) Testability

The RCW and RSW System have the capability of being tested during normal plant operation.

RCW System control and logic circuits can be individually checked by applying test or calibration signals and observing the system response. The control circuitry is designed to restore the system to the required operation if a LOCA occurs during a test.

(h) Environmental Considerations

The only control components pertinent to the RCW system that are located inside the primary containment are NBS sensors that generate signals for the LOCA signal logic. Refer to Section 3.11 for environmental qualifications of this equipment.

(i) Safety Interfaces

The safety interfaces for the RCW System Division I, II, and III controls are as follows:

— LOCA signals to Division I, II, and III RCW pumps.

— Divisions I, II and III RCW pump manual start signals from the main control room (MCR) and Divisions I and II RCW pump manual start signal from the Remote Shutdown System (RSS).

— Division I, II and III RCW pump running signals to the MCR and Divisions I and II RCW pump running signals to the RSS.

— Division I, II, and III RCW flow signals to the MCR and Divisions I and II RCW flow signal to the RSS.

— RSW A or D strainer differential pressure MCR annunciator.

— Overload and power failure signals from all RCW and RSW pumps to the MCR annunciator.

— RCW surge tank low and high level signals to the MCR annunciator.

— RCW cooling water high temperature signals to the MCR annunciator.

(j) Operational Considerations

The RCW and RSW Systems are capable of operating at a variety of cooling load conditions as required for all plant operating modes, including normal and emergency conditions.

Cooling water is required for the operation of the RHR, HECW, FPC, CAM, and Emergency Diesel Generator Systems.

When the plant is in the hot standby or cooldown mode, safety-related RCW cooling water is required for the RHR heat exchangers. Refer to Subsection 7.3.1.1.4 for a discussion of the manual or automatic operation of the RHR heat exchanger inlet and outlet isolation valves.

Process operating parameters and equipment status information are provided in the control room for the operator to accurately assess system performance. Alarms are also provided to indicate malfunction in the system. Refer to IBD Figure 7.3-7 for specific indication of equipment status in the control room. Chapter 16 describes the methods for calculating setpoints and margins.

(k) Parts of System Not Required for Safety

The non-safety-related portions of the RCW System include the annunciators and the PCF. Other instrumentation considered non-safety-related are those indicators that are provided for operator information, but are not essential to correct operator action.

7.3.1.1.8 Essential HVAC Systems—Instrumentation and Controls

See Subsections 9.4.1 and 9.4.5.

7.3.1.1.9 HVAC Emergency Cooling Water System—Instrumentation and Control

(1) System Identification

The HVAC Emergency Cooling Water System (HECW) supplies demineralized chilled water to the cooling coils of the control building safety-related electrical equipment rooms and main control room coolers, and the diesel generator zone air conditioning systems. The system is composed of three divisions, each containing two chillers and chilled water pumps.

The Control Building Chilled Water System instrumentation and controls are shown on P&ID Figure 9.2-3 and the corresponding logic on Figure 7.3-9.

(2) Support Systems (Power Source)

The instrumentation and controls of the HECW System are supplied with 120 VAC and 125 VDC electric power from Division I, II, and III power buses.

(3) Equipment Design

The HECW System consists of three mechanically (and electrically) separate systems—Divisions A, B, and C. The system is designed to provide chilled water to the cooling coils of the Control Building Control Room Habitability Area HVAC and Safety-related Equipment Area HVAC and Reactor Building Safety-related Electrical Equipment HVAC Systems.

The HECW System is designed to operate during both accident conditions and normal plant operation and during all modes of operation for the cooling systems it serves.

Each division of the HECW System consists of two chilled water pumps and chiller units; each chiller unit includes the condenser, evaporator, centrifugal compressor, refrigerant piping and package chiller controls. The system condenser is cooled by the RCW System.

Lack of flow of Reactor Building cooling water to the refrigerant condenser automatically stops the chiller. Supply flow is controlled by the condensing pressure of the refrigerant. A flow switch provided at the chilled water line shuts down the chiller and chilled water pump upon indication of low flow in the chilled water line.

(a) Initiating Circuits

The HECW System operation is initiated automatically when the controls in the main control room are set for automatic operation and any of the HVAC systems it serves are started. The HECW System can also be started manually from the main control room.

(b) Logic and Sequencing

The standby unit (chiller and chilled water pump) in Division A is automatically initiated when the operating unit is shut down. In Divisions B and C, any unit on standby is automatically initiated when any of the other operating units in Divisions B or C is stopped.

(c) Bypass and Interlocks

Low and high surge tank level switches actuate the demineralized water makeup or supply valves. Low-low or high-high surge tank level initiates an alarm in the control room to indicate a leak or a failure in the level control loop.

Flow switches provided on the chilled water line are interlocked to automatically shut down the chiller in the event of low flow in the chilled water line. A common trouble alarm for each chiller unit is annunciated in the control room upon detection of any chiller unit alarm or trip. A running signal from each RCW pump in each division is interlocked to trip the chillers if at least one RCW pump is not operating.

Each chiller unit when on standby is interlocked to automatically start as described in (b).

The running chiller is interlocked to trip on abnormal operating conditions such as lack of flow of chilled water and chiller package trouble.

(d) Redundancy and Diversity

The Control Room Habitability Area, Chilled Water System is divided into two completely independent and functionally redundant systems. Physical and electrical separation is maintained between the two redundant systems.

(e) Actuated Devices

One chiller and chilled water pump in each division is running at all times during all modes of plant operation.

The chilled water pumps and chiller units are started automatically or by remote manual switch. Status lights in the control room are also provided for this equipment.

High and low surge tank level switches actuate the opening and closing of the demineralized water makeup valve and high-high and low-low tank level switches annunciate an alarm in the control room.

The chiller capacity is controlled to maintain the chilled water temperature at the chiller outlet constant. This is done by adjusting the suction valve and hot-gas bypass within the chiller.

(f) Separation

The instrumentation, controls, and sensors of each operating division have sufficient physical and electrical separation to prevent environmental, electrical, or physical accident consequences from inhibiting the systems from performing each protective action. Physical separation is maintained by use of separate cabinets and racks for each division, and by housing redundant chiller equipment in separate cubicles.

Electrical separation is maintained by separate independent sensors and circuitry.

(g) Testability

Manual initiation of the HECW System is possible from the control room. Redundant standby components can be periodically tested, manually, to ensure system reliability while the other system is operating.

Surge tank operation can be checked by varying the tank level and observing the level at which the demineralized water makeup valve starts to open and close and when the level alarm annunciates. Automatic initiation of the standby system can be tested by simulating the trip action of the operating chiller system.

All motor-operated valves can be independently checked by operating the respective manual switch in the control room and observing the corresponding position indicator.

System chilled water flow rate and temperature can be checked by readout of locally mounted pressure and temperature gauges at the main control panel.

(h) Environmental Consideration

All components of the HECW System are selected in consideration of the normal and accident environment in which it must operate. The control equipment is seismically qualified and environmentally classified, as discussed in Sections 3.10 and 3.11.

(i) Operational Consideration

The HECW System operation is initiated in the control room by a manual master control switch. Once the system is started, it will continuously operate under all modes of plant operation to supply chilled water to the cooling coils.

Running lights, alarms, flow and temperature indicators, and valve position indicators are available in the control room for the operator to accurately monitor the HECW System operation. Chilled water pumps have running lights. A common trouble alarm is provided for each chiller unit. Surge tank high-high and low-low levels are alarmed. Motor-operated valves have position indicators. Chilled water flows have position indicators.

7.3.1.1.10 High Pressure Nitrogen Gas Supply System—Instrumentation and Controls

(1) System Identification

The High Pressure Nitrogen Gas Supply (HPIN) System provides compressed nitrogen of the required pressure to the ADS SRVs, the MSIVs (for testing only), instruments and pneumatically operated valves in the PCV and other nitrogen-using components in the reactor building (see P&ID in Figure 6.7-1 and the interconnection block diagram in Figure 7.3-10).

(2) Support Systems (Power Source)

The safety-related portion of the HPIN System is powered from the onsite Class 1E AC and DC systems. HPIN System, Division A, is powered from Class 1E Division I and HPIN System Division B is powered from Class 1E Division II. The safety-related portion is switched automatically to the standby AC power supply during a loss of normal power. The non-safety-related portion is connected to the normal AC power supply.

(3) Equipment Design

The HPIN System is separated into non-safety-related and safety-related sections.

The non-safety-related portion of the system includes an inlet filter, piping, and valves to all nitrogen users.

The safety-related portion of the system includes two banks of high pressure nitrogen bottles and associated piping, valves, and controls.

When low nitrogen gas pressure is detected in the lines to the ADS accumulators, the safety-related portion of the system is isolated from the non-safety-related portion by isolation valves which automatically cut off the normal nitrogen gas supply and open the emergency nitrogen gas bottle supply to the ADS accumulators.

In addition to valves that isolate non-safety-related equipment from safety-related equipment, the HPIN System is provided with containment isolation valves where the HPIN System lines enter the containment.

The valves are manually operated from individual control switches in the control room.

(a) Initiating Currents

During normal operation, nitrogen gas pressure is controlled and measured in a pressure control valve followed by a pressure transmitter. The pressure control valve setpoint is high enough to ensure that adequate nitrogen pressure is delivered to all the served accumulators and valves.

Automatic closure of the isolation valve from the normal nitrogen gas supply and the opening of the isolation valve from the emergency nitrogen gas bottle is initiated by low nitrogen pressure sensed in the lines to the ADS accumulators.

(b) Logic and Sequencing

The initiation of the flow of nitrogen gas from the high pressure storage bottles is by low pressure in the lines to the ADS accumulators. Concurrently, the valves isolating the non-safety-related portion of the system are closed. No other signals are required.

(c) Bypasses and Interlocks

The isolation valves on HPIN System lines serving systems in the containment have motor operators. The isolation valves may be closed to prevent any

possible leakage from the containment if a leak occurs in the system outside of the containment.

(d) Redundancy and Diversity

The HPIN System is separated into two mechanically and electrically independent divisions. Each division has instrumentation, controls, and power sources which are separated and independent from each other. One division supplies emergency nitrogen to four ADS valve accumulators, and the other division supplies emergency nitrogen to the remaining four ADS valves. This level of redundancy is sufficient because only the initial LOCA depressurization requires more than four ADS valves, and the Class 1E accumulators have sufficient capacity for one valve operation at drywell design pressure and five valve actuations at normal drywell pressure.

The HPIN storage bottles are in two racks separated from each other. Additionally, in each rack there are two banks of five bottles each. One bank is in service and the second is in standby.

(e) Actuated Devices

Nitrogen is admitted to the system and the non-safety-related portion isolated by operating valves controlled by pressure switches in the HPIN System. These valves can also be operated from the main control room.

All isolation valves can be manually operated from the main control room. Each valve is provided with indicating position lights in the main control room which verify the open and closed positions of the valve.

(f) Separation

The HPIN System is separated into two divisions, each having storage bottles and racks and piping to the ADS accumulators.

Physical separation of Division A and Division B systems is obtained by closing valves which interconnect the divisions during normal operation.

Electrical separation is maintained by separate sensors and circuits independent of each other.

(g) Testability

The HPIN System can be tested at any time by isolating the system from the normal nitrogen source and allowing the nitrogen pressure to decrease. At the proper pressure, valves will open, admitting nitrogen from the high pressure

storage bottles; other valves will close, isolating the non-safety-related portions of the system.

(h) Environmental Considerations

The system safety-related equipment is selected in consideration of the normal and accident environments in which it must be operated.

(i) Operational Considerations

The HPIN System, when required for emergency conditions, is initiated automatically with no operator action required.

Running lights, valve positions, indicating lights, and alarms are available in the control room for the operator to accurately assess the HPIN System operation. Common trouble alarms are available in the main control room for the system. Isolation valves have indicating lights for full-open and full-closed positions.

7.3.1.1.11 Not Used

7.3.1.2 Design Basis Information

IEEE-603 defines the requirements for safety systems designations and the safety systems criteria (Sections 4 and 5). The following nine paragraphs fulfill this requirement for systems and equipment described in this section.

(1) Conditions

The plant conditions which require protective action involving the systems of this section and other sections are examined in Chapter 15.

(2) Variables

The plant variables that are monitored to provide automatic protective actions are discussed in the initiating circuits sections for each system. For additional information, see Chapter 15, where safety analysis parameters for each event are cited.

(3) Number of Sensors and Location

There are no sensors in the LDS or ECCS, which have a spatial dependence, and, therefore, location information is not relevant. The only sensors used to detect essential variables of significant spatial dependence are the neutron flux detectors [Subsection 7.2.2.1(6)], the Suppression Pool Temperature Monitors [Subsection 7.6.1.7], and the radiation detectors of the Process Radiation Monitoring System.

These are in Section 7.6. All other systems discussed in Section 7.3 have sensors which have no spatial dependence.

(4) Operational Units

Prudent operational limits for each safety-related variable trip setting are selected to be far enough above or below normal operating levels so that a spurious ESF System initiation is avoided. Analysis then verifies that the release of radioactive materials, following postulate gross failures of the fuel or the nuclear system process barrier, is kept within established limits. Operational limits contained in the Technical Specifications for the ECCS and LDS are based on operating experience and constrained by the safety design basis and the safety analyses.

(5) Margin Between Operational Limits

The methods for calculating the margin between operational limits and the limiting conditions of operation for the ESF System instruments are described in Chapter 16. The margin includes the consideration of sensor and instrument channel accuracy, response times, and setpoint drift.

Indicators are provided to alert the reactor operator of the onset of unsafe conditions.

(6) Range of Energy Supply and Environmental Conditions of Safety-Related Systems

See Section 3.11 for environmental conditions and Chapter 8 for the range of energy supply conditions.

ECCS 125 VDC power is provided by the four divisions of station batteries. ECCS 120 VAC power is provided by the SSLC buses.

ESF systems motor-operated valve power is supplied from motor control centers.

(7) Malfunctions, Accidents, and Other Unusual Events Which Could Cause Damage to Safety-Related Systems

Chapter 3 covers the description of the following single credible accidents and events: flood, storm, tornado, earthquake, fire, LOCA, pipe break outside containment, and feedwater line break. Each of these events is discussed below for the ESF Systems and ECCS.

(a) Flood

The buildings containing ESF Systems and ECCS components have been designed to meet the probable maximum flood (PMF) at the site location. This ensures that the buildings will remain watertight under PMF conditions including wind-generated wave action and wave runup.

(b) Storm (Tornado)

The buildings containing ESF components have been designed to withstand meteorological events described in Subsection 3.3.2.

Superficial damage may occur to miscellaneous station property during a postulated tornado, but this will not impair the protection system capabilities.

(c) Earthquake

The structures containing ESF components have been seismically qualified (Sections 3.7 and 3.8) and will remain functional during and following a safe shutdown earthquake (SSE). Seismic qualification of instrumentation and electrical equipment is discussed in Section 3.10.

(d) Fire

To protect ESF Systems in the event of a postulated fire, the redundant portions of the systems are separated by fire barriers. If an internal fire were to occur within one of the sections of a main control room panel or in the area of one of the local panels, the ESF System functions would not be prevented by the fire. The use of separation and fire barriers ensures that, even though some portion of the system may be affected, the ESF System will continue to provide the required protective action. The Remote Shutdown System provides redundancy in the event of significant exposure fires in the control room.

The plant Fire Protection System is discussed in Section 9.5.

(e) LOCA

The following ESF System instrument taps and sensing lines are located inside the drywell and terminate outside the drywell. They could be subjected to the effects of a design basis LOCA:

— Reactor vessel pressure

— Reactor vessel water level

— Drywell pressure

These items have been environmentally qualified to remain functional during and following a LOCA (Section 3.11).

(f) Pipe Break Outside Containment and Feedwater Line Break

For any postulated pipe rupture, the structural integrity of the containment structure is maintained. In addition, SRVs and the RCIC System steamline are

located and restrained so that a pipe failure would not prevent depressurization. Separation is provided to preserve the independence of the low-pressure flooder (LPFL) systems.

For high-energy piping systems penetrating through the containment, such as the feedwater lines, isolation valves are located as close to the containment as possible. The pressure, water level, and flow sensor instrumentation for essential systems, which are required to function following a pipe rupture, are protected.

Pipe whip protection is detailed in Section 3.6.

(8) Minimum Performance Requirements

The instrumentation and control for the various systems described in this section shall, as a minimum, initiate safety action in a sufficient number of systems and subsystems to accomplish timely initiation of any required safety function under conditions of a single design basis event with its consequential damages and a single failure together with its consequential damages.

Trip points are within the operating range of instruments with full allowance for instrument error, drift, and setting error.

7.3.1.3 System Drawings

A list of the drawings is provided in Section 1.7. P&IDs are provided within Chapters 5, 6, and 9, and are referenced where appropriate in Chapter 7. All other diagrams, tables, and figures are included in Chapter 7 as appropriate. Subsection 1.7.2 provides keys for the interpretation of symbols used in these documents.

7.3.2 Analysis

7.3.2.1 Emergency Core Cooling Systems—Instrumentation and Controls

7.3.2.1.1 General Functional Requirements Conformance

Chapters 15 and 6 evaluate the individual and combined capabilities of the emergency cooling systems. For the entire range of nuclear process system break sizes, the cooling systems provide adequate removal of decay heat from the reactor core.

Instrumentation for the ECCS must respond to the potential inadequacy of core cooling regardless of the location of a breach in the reactor coolant pressure boundary. Such a breach inside or outside the containment is sensed by reactor low water level. The reactor vessel low water level signal is the only ECCS initiating function that is completely independent of breach location. Consequently, it can actuate the HPCF, RCIC, ADS and LPFL Systems.

The other major initiating function—drywell high pressure—is provided because pressurization of the drywell will result from any significant nuclear system breach anywhere inside the drywell.

Initiation of the Automatic Depressurization Subsystem (ADS) occurs when reactor vessel water below Level 1 and drywell high pressure are sensed, or when the drywell high pressure bypass timer initiated by RPV Level 1 water level runs out. Therefore it is not required that the nuclear system breach be inside the containment. This control arrangement is satisfactory in view of the automatic isolation of the reactor vessel for breaches outside the drywell and because the ADS is required only if the HPCF and/or RCIC System fail to maintain adequate reactor water level.

No operator action is required to initiate the correct responses of ECCS. However, the control room operator can manually initiate every essential operation of the ECCS. Alarms and indications in the control room allow the operator to assess situations that require the ECCS and verify the responses of each system. This arrangement limits safety dependence on operator judgment, and design of the ECCS control equipment has appropriately limited response.

The redundancy of the control equipment for the ECCS is consistent with the redundancy of the cooling systems themselves. The arrangement of the initiating signals for the ECCS is also consistent with the arrangement of the systems themselves.

No failure of a single initiating trip channel can prevent the start of the cooling systems when required or inadvertently initiate these same systems.

The control schemes for each ECCS component are designed such that no single control failure can prevent the combined cooling systems from providing the core with adequate cooling This is due to the redundancy of components and cooling systems (i.e., HPCF, RCIC, ADS, and the three divisions of LPFL).

The control arrangement used for the ADS is designed to avoid spurious actuation (Figure 7.3-2). The ADS relief valves are controlled by two trip systems per division, both of which must be in the tripped state to initiate depressurization. Within each trip system, both drywell pressure high trip or time out of the drywell high pressure bypass timer and Level 1 reactor water level trip are required to initiate a trip system.

The only equipment protective devices that can interrupt planned ECCS operation are those that must act to prevent complete failure of the component or system. In no case can the action of a protective device prevent other redundant cooling systems from providing adequate cooling to the core.

Controls for ECCS are located in the control room and are under supervision of the control room operator.

The environmental capabilities of instrumentation for the ECCS are discussed in the descriptions of the individual systems. Components that are located inside the drywell and are essential to ECCS performance are designed to operate in the drywell environment resulting from a LOCA. Safety-related instruments located outside the drywell are also qualified for the environment in which they must perform their safety-related function.

Special consideration has been given to the performance of reactor vessel water level sensors, pressure sensors, and condensing chambers during rapid depressurization of the nuclear system (see Reference 7.3-1).

Effectiveness of emergency core cooling following a postulated accident may be verified by observing the following indications:

(1) Annunciators and status lights for HPCF, RCIC, LPFL, and ADS sensor initiation logic trips

(2) Flow and pressure indications for each ECCS

(3) Valve position lights indicating open or closed valves

(4) Relief valve positions indicated by individual position sensors and discharge pipe temperature monitors

(5) Performance monitoring system logging of trips in the emergency core cooling network

The mechanical aspects of ECCS are discussed in Section 6.3.

7.3.2.1.2 Specific Regulatory Requirements Conformance

Table 7.1-2 identifies the ECCS and the associated codes and standards applied in accordance with the Standard Review Plan. The following analysis lists the applicable criteria in order of the listing on the table, and discusses the degree of conformance for each. Any exceptions or clarifications are so noted.

(1) 10CFR50.55a (IEEE-603):

The ECCS incorporates two divisions of HPCF, one division of steam-driven RCIC, two divisions of ADS and three divisions (three loops) of LPFL (RHR/low pressure flooders). This automatically actuated network of Class 1E redundant high pressure and low pressure systems assures full compliance with IEEE-603.

All components used for the ECCS are qualified for the environments in which they are located (Sections 3.10 and 3.11). All systems which make up the ECCS network are actuated by two-out-of-four logic combinations of sensors which monitor drywell pressure and reactor water level. There are a total of eight wide range water level

sensors and four drywell pressure sensors which are supplied by the Nuclear Boiler System. These instruments are shared by the ECCS as well as the RPS and other systems which require actuation signals from these essential variables. However, each system receives all four signals as input to its own unique voting logic incorporated in the ESF Logic and Control System (ELCS) network. If individual channels are bypassed for service or testing, the voting logic reverts to two-out-of-three.

The containment is divided into four quadrants, each housing the electrical equipment which, in general, corresponds to the mechanically separated division assigned to each section (i.e., mechanical divisions A, B, C, and D correspond with electrical Divisions I, II, III, and IV, respectively). Some exceptions are necessary where a given mechanical division has more than one electrical division within the quadrant. For example, the ADS valves have redundant solenoid operators which require separate divisional power interfaces. However, electrical separation is maintained between the redundant divisions.

Each of these electrical divisions contains one of the drywell pressure sensors and two of the reactor water level sensors which contribute to the two-out-of-four voting logic. All of these signals are transmitted through fiber-optic medium before entering the voting logic of the redundant divisions involved in the systems which make up the ECCS network. Separation and isolation is thus preserved both mechanically and electrically in accordance with IEEE-603 and Regulatory Guide 1.75.

Other requirements of IEEE-603, such as testing, bypasses, manual initiation, logic seal-in, etc., are described in Subsection 7.3.1.1.1.

(2) General Design Criteria (GDC)

In accordance with the Standard Review Plan for Section 7.3 and with Table 7.1-2, the following GDCs are addressed for the ECCS:

(a) **Criteria:** GDCs 2, 4, 13, 15, 19, 20, 21, 22, 23, 24, 29, 33, 34, and 35.

(b) **Conformance:** The ECCS is composed of a network of four subsystems. These are identified and described in Paragraph (1) above. The ECCS is in compliance as a whole, or in part as applicable, with all GDCs identified in (a) as discussed in Subsection 3.1.2.

The following clarification should be made with respect to GDC 23: The RPS is designed to fail in a safe state (i.e., deenergize to actuate). This is also true for the MSIVs. However, the ECCS is diverse in that it requires power to operate (i.e., energize to actuate).

The ECCS cannot be designed to provide emergency reactor coolant without electrical power. However, the two-out-of-four sensor logic and the three electrical and mechanical divisions assure that no single failure can cause ECCS failure, when required, or inadvertent initiation of ECCS. In addition, all three electrical divisions are backed up by independent onsite emergency diesel generators capable of providing full ECCS loads in the event of loss of offsite power.

(3) Regulatory Guides (RGs)

In accordance with the Standard Review Plan for Section 7.3, and with Table 7.1-2, the following RGs are addressed for the ECCS:

(a) RG 1.22—“Periodic Testing of Protection System Actuation Functions”

System logic and component testing capabilities are provided to enable fullflow testing during reactor operation as described in Subsection 7.3.1.1.1. The ECCS fully complies with this regulatory guide using the following two clarifying interpretations:

(i) Periodic testing is interpreted to mean testing of actuation devices but not to include testing of the actuated equipment which is tested during surveillance testing.

(ii) Each bypass condition shall be automatically annunciated on a trip system basis (i.e., each channel does not require separate annunciation).

(b) RG 1.47—“Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems”

The ECCS fully meets the requirements of RG 1.47. Automatic indication is provided in the control room to inform the operator that a system is inoperable. Annunciation is provided to indicate that either a system or a part of a system is not operable. For example, the ECCS has annunciator alarms whenever one or more channels of an input variable are bypassed. The operator may manually actuate the out-of-service annunciator to cover situations which cannot be automatically annunciated.

(c) RG 1.53—“Application of the Single-Failure Criterion to Nuclear Power Protection Systems”

The ECCS generally meets the requirements of RG 1.53 in addition to Section 5.1 of IEEE-603 and IEEE-379. However, specific exception is taken with regard to Paragraph C-2 as follows: Specific items which cannot be energized for test during plant operation, or tested by other than continuity tests

without degrading plant operability or safety, will be exempt from the requirements of this paragraph.

Redundant sensors and logic are utilized as described in Paragraph (1) above. There are no mode switches associated with the ECCS.

(d) RG 1.62—“Manual Initiation of Protective Actions”

All subsystems (i.e., HPCF, RCIC, ADS, and RHR/LPFL) have individual manual actuation pushbuttons with rotating collars in logic “and” combinations. The ADS has one manual start switch per channel. Thus, two collars must be rotated and two buttons pushed to actuate one division of ADS. An annunciator warning occurs when the collars are rotated. These design characteristics assure manual start to be a deliberate act. In addition, each pump has a manual start switch and each safety/relief valve has a manual keylock operation switch. There are no interlocks between the manual actuation switches and their actuation operators. The ECCS fully complies with this regulatory guide.

(e) RG 1.75-“Physical Independence of Electric Systems”

The ECCS is in compliance with this regulatory guide assuming clarifications and alternates described in Subsection 7.1.2.10.5. Separation within the ECCS is such that controls, instrumentation, equipment, and wiring is segregated into four separate divisions designated I, II, III, and IV. Sensor input signals are in Division I, II, III, and IV. Control logic is performed in Divisions I, II and III. Control and motive power separation is maintained in the same manner. Separation is provided to maintain the independence of the four divisions of the circuits and equipment so that the protection functions required during and following any design basis event can be accomplished.

All redundant equipment and circuits within the ECCS require divisional separation. All pertinent documents and drawings identify in a distinctive manner separation and safety-related status for each redundant division.

Redundant circuits and equipment are located within their respective divisional safety class enclosures. Separation is achieved by barriers, isolation devices and/or physical distance. This type of separation between redundant systems assures that a single failure of one system will not affect the operation of the other redundant system.

The separation of redundant Class 1E circuits and equipment within the ECCS is such that no physical connections are made between divisions except through nonmetallic fiber-optic medium.

Associated circuits are in accordance with Class 1E circuit requirements up to and including the isolation devices. Circuits beyond the isolation devices do not again become associated with Class 1E circuits.

Separations between Class 1E and non-Class 1E circuits either meet the same minimum requirements as for separation between Class 1E circuits or they are treated as associated circuits.

(f) [*RG 1.105—"Instrument Setpoints for Safety-Related Systems"*]*

The setpoints used for ECCS are established using a methodology consistent with this guide (Subsection 7.1.2.10.9). [*Reference 7.3-2 provides the detailed description of this methodology.*]*

(g) RG 1.118—"Periodic Testing of Electric Power and Protection Systems"

The ECCS design is consistent with the requirements of Regulatory Guide 1.118 assuming the clarifications identified in Subsection 7.1.2.10.10.

(4) Branch Technical Positions (BTP)

In accordance with the Standard Review Plan for Section 7.3, and with Table 7.1-2, the following BTPs are addressed for the ECCS:

(a) BTP ICSB 3—"Isolation of Low Pressure Systems from the High Pressure Reactor Coolant System"

Item B-5 of this BTP provides exception to the recommendations for the ECCS. However, the RHR/LPFL injection lines are designed consistent with Item B-3 in that a check valve is in series with the motor-operated injection valve (see RHR P&ID, Figure 5.4-10).

The Nuclear Boiler System provides reactor pressure sensors, one from each electrical division, which are arranged in two-out-of-four logic permissives to automatically close the LPFL injection valves should reactor pressure exceed the low pressure system design pressure. Therefore, the ECCS is in full compliance with this BTP.

(b) BTP ICSB 20—"Design of Instrumentation and Controls Provided to Accomplish Changeover from Injection to Recirculation Mode"

The ABWR, as with the BWR, has entirely separate systems for vessel injection and for vessel recirculation. Therefore, this BTP is not applicable to the ABWR.

* See Subsection 7.1.2.10.9.

(c) BTP ICSB 21—“Guidance for Application of Regulatory Guide 1.47”

The ABWR design is a single unit. Therefore, item B-2 of the BTP is not applicable. Otherwise, the ECCS is in full compliance with this BTP.

(d) BTP IGSB 22—“Guidance for Application of Regulatory Guide 1.22”

In general, actuated equipment within the reactor protection system can be fully tested during reactor operation. Exceptions for the RPS scram function are discussed in Subsection 7.2.2.2.3.1 (10). Exceptions for ECCS include the LPFL shutdown valves which cannot be opened while the reactor is pressurized. However, these can be tested during reactor shutdown.

(5) TMI Action Plan Requirements (TMI)

In accordance with the Standard Review Plan for Section 7.3, and with Table 7.1-2, the following TMIs are considered applicable for the ECCS:

(a) TMI II.D.3—“Relief and Safety Valve Position Indication”

(b) TMI II E.4.2—“Containment Isolation Dependability Positions”

(c) TMI II.K.3(13)—“HPCI and RCIC Initiation Levels”

(d) TMI II.K.3(15)—“HPCI and RCIC Initiation Levels”

(e) TMI II.K.3(15)—“Isolation of HPCI and RCIC”

(f) TMI II.K.3(18)—“ADS Actuation”

(g) TMI II.K.3(21)—“Restart of LPCS and LPCI”

(h) TMI II.K.3(22)—“RCIC Automatic Switchover”

These and all other TMI action plan requirements are addressed in Appendix 1A.

7.3.2.2 Leak Detection and Isolation System—Instrumentation and Controls

7.3.2.2.1 General Functional Requirements Conformance

The Leak Detection And Isolation System (LDS) is analyzed in this subsection. This system is described in Subsection 7.3.1.1.2, and that description is used as the basis for this analysis. The safety design bases and specific regulatory requirements of this system are stated in Section 7.1.

The isolation function of the LDS in conjunction with other safety systems, is designed to provide timely protection against the onset and consequences of the gross release of radioactive materials from fuel and reactor coolant pressure boundaries. Chapter 15 identifies and evaluates postulated events that can result in gross failure of fuel and reactor coolant pressure boundaries. The consequences of such gross failures are described and evaluated. Chapter 15 also evaluates a gross breach in a main steamline outside the containment during operation at rated power. The

evaluation shows that the main steamlines are automatically isolated in time to prevent the loss of coolant from being great enough to allow uncovering of the core. These results are true even if the longest closing time of the valve is assumed.

7.3.2.2.2 Specific Regulatory Requirements Conformance

Table 7.1-2 identifies the LDS and the associated codes and standards applied in accordance with the Standard Review Plan. The following analysis lists the applicable criteria in order of the listing on the table, and discusses the degree of conformance for each. Any exceptions or clarifications are so noted.

(1) 10CFR50.55a (IEEE-603)

The LDS sensors and Digital Trip Functions (DTFs) are arranged as a four-division system which is redundantly designed so that failure of any single element will not interfere with a required detection of leakage or isolation.

All components used for the safety isolation functions are qualified for the environments in which they are located (Sections 3.10 and 3.11). Most initiation parameters are represented by all four divisions which actuate the isolation functions via two-out-of-four logic permissives. Most of the sensors are provided by the Nuclear Boiler System. These instruments are shared by the ECCS, as well as the RPS and other systems which require actuation signals from these essential variables. However, each system receives all four signals as input to its own unique voting logic incorporated in the Reactor Trip and Isolation System (RTIS) and the ESF Logic and Control (ELCS) systems. If individual channels are bypassed for service or testing, the voting logic reverts to two-out-of-three.

The containment is divided into four quadrants, each housing the electrical equipment which, in general, corresponds to the mechanically separated divisions assigned to each section (i.e., mechanical divisions A, B, C, and D correspond with electrical Divisions I, II, III and IV, respectively). Some exceptions are necessary where a given mechanical division has more than one electrical division within the quadrant. For example, the MSIVs have redundant solenoid operators which require separate divisional power interfaces. However, electrical separation is maintained between the redundant divisions.

All of these signals are passed through fiber optic medium before entering the voting logic of the redundant divisions involved in the isolation valve logic. Separation and isolation are thus preserved both mechanically and electrically in accordance with IEEE-603 and Regulatory Guide 1.75. For further information see Subsection 9A.5.5.7.

Other requirements of IEEE-603 such as testing, bypasses, manual initiation, logic seal-in, etc., are described in Subsection 7.3.1.1.2.

(2) General Design Criteria (GDC)

In accordance with the Standard Review Plan for Section 7.3, and with Table 7.1-2, the following GDCs are addressed for the LDS:

(a) **Criteria:** GDCs 2, 4, 13, 16, 19, 20, 21, 22, 23, 24, 29, 34, 35, 38, 41, and 44.

(b) **Conformance:** The LDS is in full compliance with all GDCs identified in (a) as discussed in Subsection 3.1.2.

The following clarification should be made with respect to GDC 23: The RPS is designed to fail in a safe state (i.e., de-energize to actuate). This is also true for most isolation valves including the MSIVs. However, the RHR and RCIC isolation valves are designed to “fail as is” in that they are motor-operated valves and require power to both open and close. In addition, should the RHR or RCIC System be in operation when valve power is lost, it is essential that these valves remain open so the systems can continue their safety functions.

(3) Regulatory Guides (RGs)

In accordance with the Standard Review Plan for Section 7.3, and with Table 7.1-2, the following RGs are addressed for the LDS:

(a) RG 1.22—“Periodic Testing of Protection System Actuation Functions”

(b) RG 1.47—“Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems”

(c) RG 1.53—“Application of the Single-Failure Criterion to Nuclear Power Protection Systems”

(d) RG 1.62—“Manual Initiation of Protective Actions”

(e) RG 1.75—“Physical Independence of Electric Systems”

(f) RG 1.97—“Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident”

(g) RG 1.105—“Instrument Setpoints for Safety-Related Systems”

(h) RG 1.118—“Periodic Testing of Electric Power and Protection Systems”

The LDS conforms with all the above listed RGs, assuming the same interpretations and clarifications identified in Subsections 7.3.2.1.2 and 7.1.2.10. A generic assessment of Regulatory Guide 1.97 is provided in Section 7.5.

(4) Branch Technical Positions (BTPs)

In accordance with the Standard Review Plan for Section 7.3, and with Table 7.1-2, only BTPs 21 and 22 are considered applicable for the LDS. They are addressed as follows:

(a) BTP ICSB 21—“Guidance for Application of Regulatory Guide 1.47”

The ABWR design is a single unit. Therefore, Item B-2 of the BTP is not applicable. Otherwise, the LDS is in full compliance with this BTP.

(b) BTP ICSB 22—“Guidance for Application of Regulatory Guide 1.22”

All actuated equipment within the LDS can be fully tested during reactor operation.

(5) TMI Action Plan Requirements (TMI)

In accordance with the Standard Review Plan for Section 7.3, and with Table 7.1-2, the following TMIs are considered applicable for the LDS:

(a) TMI II.E.4.2—“Containment Isolation Dependability Positions”

(b) TMI II.F.3—“Instrumentation for Monitoring Accident Conditions”

These and all other TMI action plan requirements are addressed in Appendix 1A.

7.3.2.3 RHR/Wetwell and Drywell Spray Mode—Instrumentation and Controls

7.3.2.3.1 General Functional Requirements Conformance

When the RHR System (Loop B and C) is in the WDSC mode, the pumps take suction from the suppression pool, pass it through the RHR heat exchangers, and inject it into the wetwell and drywell atmosphere.

In the event that wetwell and/or drywell pressure exceeds a predetermined limit, after a predetermined interval following a LOCA, the RHR System flow may be manually diverted to the wetwell and drywell spray mode. The flow of the RHR pump will pass through the wetwell and drywell spray nozzles, to quench any steam and cool noncondensables in the interval following a LOCA.

7.3.2.3.2 Specific Regulatory Requirements Conformance

Table 7.1-2 identifies the WDSC mode of the RHR System and the associated codes and standards applied in accordance with the Standard Review Plan. The following analysis lists the

applicable criteria in order of the listing on the table, and discusses the degree of conformance for each. Any exceptions or clarifications are so noted.

(1) 10CFR50.55a (IEEE-603)

The WDSC mode of the RHR System is a two-loop, two-division system which is redundantly designed so that failure of any single element will not interfere with the required safety action of the system.

All components used for the safety functions are qualified for the environments in which they are located (Sections 3.10 and 3.11). The Drywell Spray mode of the RHR System (unlike the LPFL mode which is automatically actuated by LOCA) can be manually actuated should high pressure conditions occur in the drywell. The Wetwell Spray mode can be initiated at any time provided the proper permissives are present.

The containment is divided in four quadrants, each housing the electrical equipment which, in general, corresponds to the mechanically separated division assigned to each section (i.e., mechanical division A, B, C, and D correspond with the electrical Divisions I, II, III, and IV, respectively). The WDSC mode utilizes mechanical Divisions B and C with electrical Divisions II and III, respectively. Electrical separation is maintained between the redundant divisions.

The suppression cooling mode pool is designed in accordance with all requirements of IEEE-603 as described in Subsection 7.3.1.1.3.

The parent RHR System annunciates activity at the loop level (i.e., “RHR LOOP A, B, C ACTIVATED”). However, the individual mode of the RHR System is not separately annunciated.

(2) General Design Criteria (GDC)

In accordance with the Standard Review Plan for Section 7.3 and with Table 7.1-2, the following GDCs are addressed for the WDSC mode:

(a) **Criteria**: GDCs 2, 4, 13, 19, 20, 21, 22, 23, 24, 29, 38, and 44.

(b) **Conformance:** The WDSC is in compliance as a whole, or in part as applicable, with all GDCs identified in (a), as discussed in Subsection 3.1.2, except GDC 20. This is because the WDSC mode is manually initiated. However, the LPFL mode of the RHR System is automatically initiated on LOCA. In addition, should the RHR System be already operating in any other mode, it will automatically return to the LPFL mode on receipt of a LOCA signal. It is the LPFL mode of the RHR System which is part of the ECCS and helps to assure fuel design limits are not exceeded.

The following clarification should be made with respect to GDC 23: The RPS is designed to fail in a safe state (i.e., deenergize to actuate). This is also true for most isolation valves, including the MSIVs. However, the RHR and RCIC isolation valves are designed to "fail as is" in that these are motor-operated vales and require power to both open and close. In addition, should the RHR or RCIC System be in operation when valve power is lost, it is essential these valves remain open so the systems can continue their safety functions.

(3) Regulatory Guides (RGs)

In accordance with the Standard Review Plan for Section 7.3, and with Table 7.1-2, the following RGs are addressed for the WDSC mode:

(a) RG 1.22— "Periodic Testing of Protection System Actuation Functions"

(b) RG 1.47— "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems"

(c) RG 1.53— "Application of the Single-Failure Criterion to Nuclear Power Protection Systems"

(d) RG 1.62— "Manual Initiation of Protective Actions"

(e) RG 1.75— "Physical Independence of Electric Systems"

(f) RG 1.105— "Instrument Setpoints for Safety-Related Systems"

(g) RG 1.118— "Periodic Testing of Electric Power and Protection Systems"

The WDSC mode conforms with all the above-listed RGs assuming the same interpretations and clarification identified in Subsections 7.3.2.1.2 and 7.1.2.10.

With regard to RG 1.105, there are no initiation setpoints, since the WDSC mode is not automatically initiated. However, an interlock is provided such that the drywell spray valves cannot be opened unless a high drywell pressure signal is present.

The wetwell spray valves do not have an interlock. The operator relies on the instrumentation that provides indication of the wetwell air space pressure condition when initiating this mode.

(4) Branch Technical Positions (BTPs)

In accordance with the Standard Review Plan for Section 7.3, and with Table 7.1-2, only BTPs 21 and 22 are considered applicable for the Wetwell / Drywell Spray mode. They are addressed as follows:

(a) BTP ICSB 21— "Guidance for Application of Regulatory Guide 1.47"

The ABWR design is a single unit. Therefore, Item B-2 of the BTP is not applicable. Otherwise, the WDSC is in full compliance with this BTP.

(b) BTP ICSB 22— "Guidance for Application of Regulatory Guide 1.22"

All actuated equipment within the WDSC mode can be fully tested during reactor operation.

(5) TMI Action Plan Requirements (TMI)

In accordance with the Standard Review Plan for Section 7.3, and with Table 7.1-2, only TMI II.E.4.2 ("Containment Isolation Dependability Positions") is considered applicable for the WDSC.

These and all other TMI action plan requirements are addressed in Appendix 1A.

7.3.2.4 RHR/Suppression Pool Cooling Mode—Instrumentation and Controls

7.3.2.4.1 General Functional Requirements Conformance

The SPC mode of the RHR System [SPC (RHR)] is designed to limit the water temperature in the suppression pool such that the temperature immediately after a blowdown does not exceed the established limit when reactor pressure is above the limit for cold shutdown. During this mode of operation, water is pumped from the suppression pool, through the RHR System heat exchangers, and back to the suppression pool. Thus, the SPC (RHR) maintains the suppression pool as a heat sink for reactor and containment blowdown and source of water for ECCS and wetwell and drywell spray.

7.3.2.4.2 Specific Regulatory Requirements Conformance

Table 7.1-2 identifies the SPC mode of the RHR System and the associated codes and standards applied in accordance with the Standard Review Plan. The following analysis lists the applicable criteria in order of the listing on the table, and discusses the degree of conformance for each. Any exceptions or clarifications are so noted.

(1) 10CFR50.55a (IEEE-603)

The SPC mode of the RHR System is a three-loop, three-division system which is redundantly designed so that failure of any single element will not interfere with the required safety action of the system.

All components used for the safety functions are qualified for the environments in which they are located (Sections 3.10 and 3.11).

The containment is divided into four quadrants, each housing the electrical equipment which, in general, corresponds to the mechanically separated divisions assigned to each section (i.e., mechanical Divisions A, B, C, and D correspond with electrical Divisions I, II, III, and IV, respectively). The SPC mode utilizes mechanical Divisions A, B, and C with electrical Divisions I, II, and III, respectively. Electrical separation is maintained between the redundant divisions.

The suppression cooling mode pool system is designed in accordance with all requirements of IEEE-603 as described in Subsection 7.3.1.1.4.

The parent RHR System annunciates activity at the loop level (i.e., “RHR LOOP A, B, C ACTIVATED”). However, the individual mode of the RHR System is not separately annunciated.

(2) General Design Criteria (GDC)

In accordance with the Standard Review Plan for Section 7.3 and with Table 7.1-2, the following GDCs are addressed for the SPC:

(a) **Criteria:** GDCs 2, 4, 13, 19, 20, 21, 22, 23, 24, 29, 38, and 44.

(b) **Conformance:** The SPC mode is in compliance, as a whole or in part, as applicable, with all GDCs identified in (a), as discussed in Subsection 3.1.2.

The following clarification should be made with respect to GDC 23: The RPS is designed to fail in a safe state (i.e., deenergize to actuate). This is also true for most isolation valves, including the MSIVs. However, the RHR and RCIC isolation valves are designed to “fail as is” in that these are motor-operated valves and require power to both open and close. In addition, should the RHR or RCIC System be in operation when valve power is lost, it is essential these valves remain open so the systems can continue their safety functions.

(3) Regulatory Guides (RGs)

In accordance with the Standard Review Plan for Section 7.3, and with Table 7.1-2, the following RGs are addressed for the SPC mode:

(a) RG 1.22— “Periodic Testing of Protection System Actuation Functions”

(b) RG 1.47— “Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems”

(c) RG 1.53— “Application of the Single-Failure Criterion to Nuclear Power Protection Systems”

(d) RG 1.62— “Manual Initiation of Protective Actions”

(e) RG 1.75— “Physical Independence of Electric Systems”

(f) RG 1.105— “Instrument Setpoints for Safety-Related Systems”

(g) RG 1.118— “Periodic Testing of Electric Power and Protection Systems”

The SPC mode complies with all the above listed RGs, except RG 1.105, assuming the same interpretations and clarifications identified in Subsections 7.3.2.1.2 and 7.1.2.10 except when the injection valve, and the suppression pool return, are in the manual override mode. The only interlock is the LOCA signal which closes the SPC valve to effect automatic transfer to the LPFL mode.

(4) Branch Technical Positions (BTPs)

In accordance with the Standard Review Plan for Section 7.3, and with Table 7.1-2, only BTPs 21 and 22 are considered applicable for the SPC mode. They are addressed as follows:

(a) BTP ICSB 21— “Guidance for Application of Regulatory Guide 1.47”

The ABWR design is a single unit. Therefore, Item B-2 of the BTP is not applicable. Otherwise, the SPC mode is in full compliance with this BTP.

(b) BTP ICSB 22— “Guidance for Application of Regulatory Guide 1.22”

All actuated equipment within the SPC can be fully tested during reactor operation.

(5) TMI Action Plan Requirements (TMI)

In accordance with the Standard Review Plan for Section 7.3, and with Table 7.1-2, only TMI II.E.4.2 (“Containment Isolation Dependability Positions”) is considered applicable for the SPC mode.

These and all other TMI action plan requirements are addressed in Appendix 1A.

7.3.2.5 Standby Gas Treatment System—Instrumentation and Controls

7.3.2.5.1 Conformance to General Functional Requirements

The Standby Gas Treatment System (SGTS) limits the release to the environment of halogens and particulates from the leakage air exhaust of the secondary containment during accident conditions.

7.3.2.5.2 Specific Regulatory Requirements Conformance

Table 7.1-2 identifies the SGTS and the associated codes and standards applied in accordance with the Standard Review Plan. The following analysis lists the applicable criteria in order of

the listing on the table, and discusses the degree of conformance for each. Any exceptions or clarifications are so noted.

(1) 10CFR50.55a (IEEE-603)

The SGTS has two electrical divisions and is redundantly designed so that failure of any electrical component will not interfere with the required safety action of the system.

Two completely redundant systems consisting of filter trains, fan, and associated piping are provided.

All components used for the safety functions are qualified for the environments in which they are located (Sections 3.10 and 3.11).

The SGTS is automatically initiated from isolation signals originating in the LDS. The system also has full manual actuation capability.

The SGTS utilizes mechanical Divisions B & C with electrical Divisions II & III, respectively. Electrical separation is maintained between the redundant divisions.

The SGTS is designed to meet all the requirements of IEEE-603. Detailed system design descriptions are given in Subsection 7.3.1.1.5.

(2) General Design Criteria (GDC)

In accordance with the Standard Review Plan for Section 7.3, and with Table 7.1-2, the following GDCs are addressed for the SGTS:

(a) **Criteria:** GDCs 2, 4, 13, 19, 20, 21, 22, 24, 29, 41 and 43.

(b) **Conformance:** The SGTS is in compliance as a whole, or in part as applicable, with all GDCs identified in (a), as discussed in Subsection 3.1.2.

(3) Regulatory Guides (RGs)

In accordance with the Standard Review Plan for Section 7.3, and with Table 7.1-2, the following RGs are addressed for the SGTS:

(a) RG 1.22— “Periodic Testing of Protection System Actuation Functions”

(b) RG 1.47— “Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems”

(c) RG 1.52— “Design, Testing and Maintenance Criteria for Post-Accident Engineered-Safety-Feature Atmosphere Cleanup Systems Air Filtration and Adsorption Units of Light-Water-Cooled Nuclear Power Plants”

(d) RG 1.53— “Application of the Single-Failure Criterion to Nuclear Power Protection Systems”

(e) RG 1.62— “Manual Initiation of Protective Actions”

(f) RG 1.75— “Physical Independence of Electric Systems”

(g) RG 1.105— “Instrument Setpoints for Safety-Related Systems”

(h) RG 1.118— “Periodic Testing of Electric Power and Protection Systems”

With regard to RG 1.53, no active component failure will result in SGTS system failure. The SGTS conforms with all the above listed RGs, assuming the same interpretations and clarifications identified in Subsections 7.3.2.1.2 and 7.1.2.10.

(4) Branch Technical Positions (BTPs)

In accordance with the Standard Review Plan for Section 7.3, and with Table 7.1-2, only BTPs 21 and 22 are considered applicable for the SGTS. They are addressed as follows:

(a) BTP ICSB 21— “Guidance for Application for Regulatory Guide 1.47”

The ABWR design is a single unit. Therefore, Item B-2 of the BTP is not applicable. Otherwise, the SGTS is in full compliance with this BTP.

(b) BTP ICSB 22— “Guidance for Application of Regulatory Guide 1.22”

All actuated equipment within the SGTS can be fully tested during reactor operation.

(5) TMI Action Plan Requirements (TMI)

In accordance with the Standard Review Plan for Section 7.3, and with Table 7.1-2, there are no TMI action plan requirements applicable to the SGTS.

7.3.2.6 Emergency Diesel Generator Support System—Instrumentation and Control

7.3.2.6.1 Conformance to General Functional Requirements

The instrumentation and controls for the diesel generator auxiliary systems are provided to monitor the temperature, pressure and level of the auxiliary system process fluids and to control the operation of system compressors, pumps, heaters and coolers. Additional information is provided in Chapter 9.

7.3.2.6.2 Specific Regulatory Requirements Conformance

Table 7.1-2 identifies the emergency diesel generator support systems with the associated codes and standards applied in accordance with the Standard Review Plan. The following analysis lists the applicable criteria in order of the listing on the table, and discusses the degree of conformance for each. Any exceptions or clarifications are so noted.

(1) 10CFR50.55a (IEEE-603)

The Emergency Diesel Generator Support System, as identified in Subsection 7.3.1.1.6, is the diesel generator jacket water system, the diesel generator starting air system, the diesel generator lubrication system, the diesel fuel transfer system, and the diesel combustion air intake and exhaust system. Redundancy is provided to assure that single failure of any electrical component will not interfere with the required safety action of more than one of three generator systems. The fuel tanks and their interfaces with the diesels is described in Chapter 9.

All components used for the safety functions are qualified for the environments in which they are located (Sections 3.10 and 3.11)

A safety analysis is provided for each support system in Chapter 9.

(2) General Design Criteria (GDC)

In accordance with the Standard Review Plan for Section 7.3, and with Table 7.1-2, the following GDCs are addressed for the diesel generator support systems:

(a) **Criteria:** GDCs 2, 4, 13, 19, and 44.

(b) **Conformance:** The diesel generator support systems are in compliance as a whole, or in part as applicable, with all GDCs identified in (a), as discussed in Subsection 3.1.2.

(3) Regulatory Guides (RGs)

In accordance with the Standard Review Plan for Section 7.3, and with Table 7.1-2, the following RGs are addressed for the diesel generator support systems.

(a) RG 1.22— “Periodic Testing of Protection System Actuation Functions”

(b) RG 1.47— “Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems”

(c) RG 1.53— “Application of the Single-Failure Criterion to Nuclear Power Protection Systems”

(d) RG 1.62— “Manual Initiation of Protective Actions”

(e) RG 1.75— “Physical Independence of Electric Systems”

(f) RG 1.105— “Instrument Setpoints for Safety-Related Systems”

(g) RG 1.118— “Periodic Testing of Electric Power and Protection Systems”

The diesel generator support systems conform with all the above listed RGs, assuming the same interpretations and clarifications identified in Subsections 7.3.2.1.2 and 7.1.2.10.

(4) Branch Technical Positions (BTPs)

In accordance with the Standard Review Plan for Section 7.3, and with Table 7.1-2, only BTPs 21 and 22 are considered applicable for the diesel generator support systems.

They are addressed as follows:

(a) BTP ICSB 21— “Guidance for Application for Regulatory Guide 1.47”

The ABWR design is a single unit. Therefore, Item B-2 of the BTP is not applicable. Otherwise, the diesel generator support systems are in full compliance with this BTP.

(b) BTP ICSB 22— “Guidance for Application of Regulatory Guide 1.22”

All actuated equipment within the diesel generator support systems can be fully tested during reactor operation.

(5) TMI Action Plan Requirements (TMI)

In accordance with the Standard Review Plan for Section 7.3, and with Table 7.1-2, there are no TMI action plan requirements applicable to the diesel generator support systems.

7.3.2.7 Reactor Building Cooling Water System and Reactor Service Water System Instrumentation and Controls

7.3.2.7.1 Conformance to General Functional Requirements

The Reactor Building Cooling Water (RCW) System and the Reactor Service Water System operate during all modes of plant operations. Should low water level occur in the RCW surge tank, all isolation valves to non-safety-related components close automatically. If the operator determines later that the non-safety-related components are operable, cooling flow can be restored by remote manual operation of the component isolation valves. If a break occurs in the Control Building Basement, water level sensors close isolation valves in the RSW system in that division.

7.3.2.7.2 Specific Regulatory Requirements Conformance

Table 7.1-2 identifies the RCW and RSW Systems and the associated codes and standards applied in accordance with the Standard Review Plan. The following analysis lists the applicable criteria in order of the listing on the table, and discusses the degree of conformance for each. Any exceptions or clarifications are so noted.

(1) 10CFR50.55a (IEEE-603)

The RCW and the RSW Systems have three independent electrical divisions and are redundantly designed so that failure of any single electrical component in a system division will not interfere with the required safety action of the affected system.

During normal operation, all divisions of the RCW and the RSW Systems supply safety-related and non-safety-related cooling loads. An RCW surge tank low level signal (two-out-of-three logic) causes the non-safety-related RCW loads except for FPC heat exchangers and FPC pump room air-conditioning units to be automatically isolated. A LOCA signal will isolate all RCW non-safety-related loads except the instrument air coolers, CRD oil coolers, FPC heat exchangers, FPC pump room air-conditioning units, service air coolers, and CUW pump motor coolers. This isolation can also be initiated manually from the control room. Neither of the above signals will affect the RSW System.

All components used for the safety-related functions are qualified for the environments in which they are located (Sections 3.10 and 3.11).

The RCW and the RSW Systems utilize mechanical Divisions A, B, and C, corresponding with electrical Divisions I, II, and III, respectively. Electrical separation is maintained between the redundant divisions in each system.

The RCW and the RSW Systems are designed to meet all applicable requirements of IEEE-603. Detailed system design descriptions are given in Subsection 7.3.1.1.7 and in Section 9.2.

(2) General Design Criteria (GDC)

In accordance with the Standard Review Plan for Section 7.3, and with Table 7.1-2, the following GDCs are addressed for the RCW System:

(a) **Criteria:** GDCs 2, 4, 13, 19, 20, 21, 22, 23, 24, 29, 34, 35, 38 and 44.

(b) **Conformance:** The RCW System is in compliance as a whole, or in part as applicable, with all GDCs identified in (a), as discussed in Subsection 3.1.2.

(3) Regulatory Guides (RGs)

In accordance with the Standard Review Plan for Section 7.3, and with Table 7.1-2, the following RGs are addressed for the RCW System:

(a) RG 1.22— “Periodic Testing of Protection System Actuation Functions”

(b) RG 1.47— “Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems”

(c) RG 1.53— “Application of the Single-Failure Criterion to Nuclear Power Protection Systems”

(d) RG 1.62— “Manual Initiation of Protective Actions”

(e) RG 1.75— “Physical Independence of Electric Systems”

(f) RG 1.118— “Periodic Testing of Electric Power and Protection Systems”

The RCW System conforms with all the above listed RGs, assuming the same interpretations and clarifications identified in Subsections 7.3.2.1.2 and 7.1.2.10.

(4) Branch Technical Positions (BTPs)

In accordance with the Standard Review Plan for Section 7.3, and with Table 7.1-2, only BTPs 21 and 22 are considered applicable for the RCW System. They are addressed as follows:

(a) BTP ICSB 21— “Guidance for Application for Regulatory Guide 1.47”

The ABWR design is a single unit. Therefore, Item B-2 of the BTP is not applicable. Otherwise, the RCW is in full compliance with this BTP.

(b) BTP ICSB 22— “Guidance for Application of Regulatory Guide 1.22”

All actuated equipment within the RCW System can be fully tested during reactor operation.

(5) TMI Action Plan Requirements (TMI)

In accordance with the Standard Review Plan for Section 7.3, and with Table 7.1-2, there are no TMI action plan requirements applicable to the RCW System.

7.3.2.8 Essential HVAC Systems—Instrumentation and Control

7.3.2.8.1 Conformance to General Functional Requirements

The Essential HVAC Systems equipment and controls provide a controlled temperature environment to ensure the continued operation of safety-related equipment under accident conditions. This equipment is located in specific areas of the Reactor and Auxiliary buildings.

7.3.2.8.2 Specific Regulatory Requirements Conformance

Table 7.1-2 identifies the HVAC Systems and the associated codes and standards applied in accordance with the Standard Review Plan. The following analysis lists the applicable criteria in order of the listing on the table, and discusses the degree of conformance for each. Any exceptions or clarifications are so noted.

(1) 10CFR50.55a (IEEE-603)

The essential HVAC Systems (HVAC) are powered by three independent electrical divisions and are redundantly designed so that failure of any single electrical component will not interfere with the required safety action of the system.

Certain non-safety-related HVAC equipment required to operate during a loss of offsite power is connected to the onsite power distribution system except when a LOCA signal exists. The balance of the non-safety-related HVAC equipment is connected to the normal offsite power distribution system.

All components used for the safety functions are qualified for the environments in which they are located (Sections 3.10 and 3.11).

The HVAC System utilizes mechanical Divisions A, B, and C corresponding with electrical Divisions I, II, and III, respectively. Electrical separation is maintained between the redundant divisions.

The HVAC System is designed to meet all applicable requirements of IEEE-603. Detailed system design descriptions are given in Subsection 7.3.1.1.8 and in Chapter 9.

(2) General Design Criteria (GDC)

In accordance with the Standard Review Plan for Section 7.3, and with Table 7.1-2, the following GDCs are addressed for the HVAC:

(a) **Criteria:** GDCs 2, 4, 13, 19, 20, 21, 22, 23, 24, and 29.

(b) **Conformance:** The HVAC System is in compliance as a whole, or in part as applicable, with all GDCs identified in (a), as discussed in Subsection 3.1.2.

(3) Regulatory Guides (RGs)

In accordance with the Standard Review Plan for Section 7.3, and with Table 7.1-2, the following RGs are addressed for the HVAC System:

(a) RG 1.22— “Periodic Testing of Protection System Actuation Functions”

(b) RG 1.47— “Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems”

(c) RG 1.53— “Application of the Single-Failure Criterion to Nuclear Power Protection Systems”

(d) RG 1.62— “Manual Initiation of Protective Actions”

(e) RG 1.75— “Physical Independence of Electric Systems”

(f) RG 1.118— “Periodic Testing of Electric Power and Protection Systems”

The HVAC conforms with all the above listed RGs, assuming the same interpretations and clarifications identified in Subsections 7.3.2.1.2 and 7.1.2.10.

(4) Branch Technical Positions (BTPs)

In accordance with the Standard Review Plan for Section 7.3, and with Table 7.1-2, only BTPs 21 and 22 are considered applicable for the HVAC System. They are addressed as follows:

(a) BTP ICSB 21— “Guidance for Application for Regulatory Guide 1.47”

The ABWR design is a single unit. Therefore, item B-2 of the BTP is not applicable. Otherwise, the HVAC System is in full compliance with this BTP.

(b) BTP ICSB 22— “Guidance for Application of Regulatory Guide 1.22”

All actuated equipment within the HVAC System can be fully tested during reactor operation.

(5) TMI Action Plan Requirements (TMI)

In accordance with the Standard Review Plan for Section 7.3, and with Table 7.1-2, there are no TMI action plan requirements applicable to the HVAC System.

7.3.2.9 HVAC Emergency Cooling Water System—Instrumentation and Control

7.3.2.9.1 Conformance to General Functional Requirements

The HVAC Emergency Cooling Water (HECW) System provides chilled water to the Control Building Safety-related Equipment Area HVAC and to the Control Room Habitability Area HVAC and Reactor Building Safety-related Electrical Equipment HVAC Systems. It is designed to function under all operating, emergency and accident conditions.

7.3.2.9.2 Specific Regulatory Requirements Conformance

Table 7.1-2 identifies the HECW System and the associated codes and standards applied in accordance with the Standard Review Plan. The following analysis lists the applicable criteria

in order of the listing on the table, and discusses the degree of conformance for each. Any exceptions or clarifications are so noted.

(1) 10CFR50.55a (IEEE-603)

The HVAC Emergency Cooling Water (HECW) System has three independent electrical divisions and is redundantly designed so that failure of any single electrical component will not interfere with the required safety action of the system.

The HECW System is manually actuated, but is designed to run continuously during reactor operation. Should a loss of station power or a LOCA event occur, the system power sources will automatically switch over to the emergency diesels. Thus, continuous operation is assured for all plant conditions.

All components used for the safety functions are qualified for the environments in which they are located (Sections 3.10 and 3.11).

The HECW System utilizes mechanical Divisions A, B and C corresponding with electrical Divisions I, II, and III, respectively. Electrical separation is maintained between the redundant divisions.

The HECW System is designed to meet all applicable requirements of IEEE-603. Detailed system design descriptions are given in Subsection 7.3.1.1.9 and in Chapter 9.

(2) General Design Criteria (GDC)

In accordance with the Standard Review Plan for Section 7.3, and with Table 7.1-2, the following GDCs are addressed for the HVAC System:

(a) **Criteria:** GDCs 2, 4, 13, 19, 20, 21, 22, 23, 24, 29, and 44.

(b) **Conformance:** The HECW System is in compliance as a whole, or in part as applicable, with all GDCs identified in (a), as discussed in Subsection 3.1.2.

(3) Regulatory Guides (RGs)

In accordance with the Standard Review Plan for Section 7.3, and with Table 7.1-2, the following RGs are addressed for the HECW System:

(a) RG 1.22— “Periodic Testing of Protection System Actuation Functions”

(b) RG 1.47— “Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems”

(c) RG 1.53— “Application of the Single-Failure Criterion to Nuclear Power Protection Systems”

(d) RG 1.62— "Manual Initiation of Protective Actions"

(e) RG 1.75— "Physical Independence of Electric Systems"

(f) RG 1.118— "Periodic Testing of Electric Power and Protection Systems"

The HECW System conforms with all the above listed RGs, assuming the same interpretations and clarifications identified in Subsections 7.3.2.1.2 and 7.1.2.10.

(4) Branch Technical Positions (BTPs)

In accordance with the Standard Review Plan for Section 7.3, and with Table 7.1-2, only BTPs 21 and 22 are considered applicable for the HECW System. They are addressed as follows:

(a) BTP ICSB 21— "Guidance for Application for Regulatory Guide 1.47"

The ABWR design is a single unit. Therefore, Item B-2 of the BTP is not applicable. Otherwise, the HECW System is in full compliance with this BTP.

(b) BTP ICSB 22— "Guidance for Application of Regulatory Guide 1.22"

All actuated equipment within the HECW System can be fully tested during reactor operation.

(5) TMI Action Plan Requirements (TMI)

In accordance with the Standard Review Plan for Section 7.3, and with Table 7.1-2, there are no TMI action plan requirements applicable to the HECW System.

7.3.2.10 High Pressure Nitrogen Gas Supply System—Instrumentation and Controls

7.3.2.10.1 Conformance to General Functional Requirements

The High Pressure Nitrogen Gas Supply (HPIN) System is capable of operating during all modes of plant operation. When low nitrogen pressure occurs, the isolation valve to the non-safety-related supply closes and isolation valves to the safety-related nitrogen supply open automatically to ensure adequate compressed nitrogen to the ADS accumulators. Restoration of the HPIN System to normal operation is by manual operation of the isolation valves from the control room.

7.3.2.10.2 Specific Regulatory Requirements Conformance

Table 7.1-2 identifies the HPIN System and the associated codes and standards applied in accordance with the Standard Review Plan. The following analysis lists the applicable criteria in order of the listing on the table, and discusses the degree of conformance for each. Any exceptions or clarifications are so noted.

(1) 10CFR50.55a (IEEE-603)

The HPIN System has two independent electrical divisions and mechanical divisions and is redundantly designed so that failure of any single electrical component will not interfere with the required safety action of the system. One division supplies emergency nitrogen to four ADS valve accumulators and the other division; to the remaining four ADS valve accumulators. This level of redundancy is adequate because only the initial LOCA depressurization requires more than four ADS valves and the Class-1E accumulators have sufficient capacity for one valve actuation at drywell design pressure and five actuations at normal drywell pressure.

All components used for the safety-related functions are qualified for the environments in which they are located (Sections 3.10 and 3.11).

The HPIN System is designed to meet all applicable requirements of IEEE-603. Detailed system design descriptions are given in Subsection 7.3.1.1.10 and in Chapter 6.

(2) General Design Criteria (GDC)

In accordance with the Standard Review Plan for Section 7.3, and with Table 7.1-2, the following GDCs are addressed for the HPIN System:

(a) **Criteria:** GDCs 2, 4, 13, 19, 20, 21, 22, 23, 24, and 29.

(b) **Conformance:** The HPIN System is in compliance as a whole, or in part as applicable, with all GDCs identified in (a), as discussed in Subsection 3.1.2.

(3) Regulatory Guides (RGs)

In accordance with the Standard Review Plan for Section 7.3, and with Table 7.1-2, the following RGs are addressed for the HPIN System:

(a) RG 1.22— “Periodic Testing of Protection System Actuation Functions”

(b) RG 1.47— “Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems”

(c) RG 1.53— “Application of the Single-Failure Criterion to Nuclear Power Protection Systems”

(d) RG 1.62— “Manual Initiation of Protective Actions”

(e) RG 1.75— “Physical Independence of Electric Systems”

(f) RG 1.118— “Periodic Testing of Electric Power and Protection Systems”

The HPIN System conforms with all the above listed RGs, assuming the same interpretations and clarifications identified in Subsections 7.3.2.1.2 and 7.1.2.10.

(4) Branch Technical Positions (BTPs)

In accordance with the Standard Review Plan for Section 7.3, and with Table 7.1-2, only BTPs 21 and 22 are considered applicable for the HPIN System. They are addressed as follows:

(a) BTP ICSB 21— "Guidance for Application for Regulatory Guide 1.47"

The ABWR design is a single unit. Therefore, Item B-2 of the BTP is not applicable.

Otherwise, the HPIN System is in full compliance with this BTP.

(b) BTP ICSB 22— "Guidance for Application of Regulatory Guide 1.22"

All actuated equipment within the HPIN System can be fully tested during reactor operation.

(5) TMI Action Plan Requirements (TMI)

In accordance with the Standard Review Plan for Section 7.3, and with Table 7.1-2, there are no TMI action plan requirements applicable to the HPIN System.

7.3.2.11 Additional Design Considerations Analyses

7.3.2.11.1 General Plant Safety Analysis

The examination of the ESF Systems at the plant safety analyses level is presented in Chapter 15.

7.3.2.11.2 Loss of Plant Instrument Air System

Loss of plant instrument air will not negate the ESF Systems safety functions (Chapter 15).

7.3.2.11.3 Loss of Cooling Water to Vital Equipment

Loss of cooling water to ECCS, containment and reactor vessel isolation systems and other systems described in this section, when subject to single active component failure (SACF) or single operator error (SOE) will not result in the loss of sufficient ESF Systems to negate their safety function (Chapter 15).

7.3.2.12 Periodic Testing of ESF Instrumentation

Protection system inservice testability is discussed in Subsection 7.1.2.1.6.

7.3.3 COL License Information

7.3.3.1 Cooling Temperature Profiles for Class 1E Digital Equipment

The COL applicant shall include, as part of its pre-operational test procedure, cooling temperature profiles for racks containing Class 1E microprocessor-designed equipment. The profiles shall include data for HVAC configurations consistent with the various accident events which require Engineered Safety Features (ESF) systems.

7.3.4 References

7.3-1 NEDO-24708, Additional Information Required for NRC Staff Generic Report on Boiling Water Reactors, September 1979.

7.3-2 [*WCAP-17119-NP(P), "Methodology for STP Units 3 and 4, ABWR Technical Specification Setpoints," Revision 2, July 2010.*]*

* See Subsection 7.1.2.10.9.

The following figures are located in Chapter 21: