7.4 Systems Required for Safe Shutdown

7.4.1 Description

This section examines and discusses the instrumentation and control aspects of the following plant systems and functions designed to assure safe and orderly shutdown of the ABWR:

(1) Alternate Rod Insertion function (ARI)

(2) Standby Liquid Control System (SLCS)

(3) Reactor Shutdown Cooling mode (RHR)

(4) Remote Shutdown System (RSS)

See Subsection 7.1.2.4 which addresses the design basis information required by Section 4 of IEEE-603.

7.4.1.1 Alternate Rod Insertion Function–Instrumentation and Controls

The alternate rod insertion (ARI) function is accomplished independently and diversely from the Reactor Protection System (RPS). The Recirculation Flow Control System (RFCS) receives isolated, low reactor level signals from the four ESF Logic and Control System (ELCS) divisions from reactor level sensors and safety controller equipment separate from that used for the RPS low reactor level SCRAM function. The RFCS also receives redundant high reactor dome pressure status signals from the non-safety Steam Bypass and Control System. The low reactor level signals and high reactor dome pressure signals are used for the RFCS logic for automatic initiation of the ARI function. In addition, the reactor operator, using two dedicated switches located on the Main Control Room Panel, can initiate the ARI function manually. When the ARI function is activated, either automatically or manually, ARI activation signals are provided to the ARI valves of the Control Rod Drive System and simultaneously to the Rod Control and Information System. Energization of the ARI valves (separate from the scram valves), causes reactor shutdown by hydraulic insertion of the control rods. The RCIS, acting upon ARI initiation signals from the RFCS, causes reactor shutdown by electromechanical insertion of control rods using the FMCRD motors.

The RCIS, including the active run-in function of the FMCRD motors and the ARI valves, are not required for safety, nor are these components qualified in accordance with safety criteria. However, the FMCRD components associated with hydraulic scram are qualified in accordance with safety criteria.

The inherent diversity of ARI provides mitigation of the consequences of anticipated transient without scram (ATWS) events.

7.4.1.2 Standby Liquid Control System–Instrumentation and Controls

(1) Function

The instrumentation and controls for the SLCS are designed to initiate and continue injection of a liquid neutron absorber into the reactor when manually or automatically called upon to do so. This equipment also provides the necessary controls to maintain this liquid chemical solution well above saturation temperature in readiness for injection. The system P&ID is shown in Figure 9.3-1. The interlock block diagram (IBD) is shown in Figure 7.4-1.

(2) Classification

The SLCS is a backup method to shut down the reactor to cold subcritical conditions by independent means other than the normal method by the CRD System. Thus, the system is considered a safe shutdown system. The SLCS process equipment, instrumentation, and controls essential for injection of the neutron absorber solution into the reactor are designed to withstand Seismic Category I earthquake loads. Any nondirect process equipment, instrumentation, and controls of the system are not required to meet Seismic Category I requirements; however, the local and control room mounted equipment is located in seismically qualified panels.

(3) Power Sources

The power supply to one motor-operated injection valve, storage tank discharge valve, and injection pump is powered from Division I, 480 VAC. The power supply to the other motor-operated injection valve, storage tank outlet valve, and injection pump is powered from Division II, 480 VAC. The power supply to the tank heaters and heater controls is connectable to a standby AC power source. The standby power source is Class 1E from an onsite source and is independent of the offsite power. The power supply to the main control room benchboard indicator lights and the level and pressure sensors is powered from a Class 1E instrument bus.

(4) Equipment

The SLCS is a special plant-capability event system. No single active component failure of any plant system or component would necessitate the need for the operational function of the SLCS. It is included for a number of special consideration events:

(a) Plant capability to shut down the reactor without control rods from normal operation (Chapter 15).

(b) Plant capability to shut down the reactor without control rods from a transient incident (Chapter 15).

Although this system has been designed to a high degree of reliability with many safety system features, it is not required to meet the safety design basis requirements of the safety-related systems.

(5) Initiating Circuits

The SLCS is automatically initiated upon receiving an ATWS signal. The SLCS is initiated manually in the main control room by turning a keylocking switch for system A or a different keylocking switch for system B to the START position.

(6) Logic and Sequencing

When one division of the SLCS is initiated, one injection valve and one tank discharge valve start to open immediately. The pump that has been selected for injection will not start until its associated tank discharge valve is at the fully open position. In order to provide maximum MOV availability when the SLCS is in normal standby readiness, the overloads for the storage tank outlet valves are bypassed by a contact from a test switch in its NORMAL position. When the TEST position is selected, the overload short is removed, thus allowing motor protection during test operation of the valves.

(7) Bypasses and Interlocks

Pumps are interlocked so that either the storage tank discharge valve or the test tank discharge valve must be fully open for the pump to run. When the SLCS is initiated to inject the neutron absorber into the reactor, the outboard isolation valves of the reactor water cleanup system automatically close.

(8) Redundancy and Diversity

Under special shutdown conditions, the SLCS is functionally redundant to the Control Rod Drive System in achieving and maintaining the reactor subcritical. Therefore, the SLCS as a system by itself is not required to be redundant, although the active components and control channels are redundant for serviceability.

The SLCS provides a diverse means for shutting down the reactor using a liquid neutron absorber in the event of a control rod drive system failure.

The method of identifying redundant power cables, signal cables, and cable trays and the method of identifying non-safety-related cables as associated circuits are discussed in Subsection 8.3.3.5.

(9) Actuated Devices

When the SLCS is automatically initiated to inject a liquid neutron absorber into the reactor, the following devices are actuated:

(a) The two injection valves are opened.

(b) The two storage tank discharge valves are opened.

(c) The two injection pumps are started.

(d) The reactor water cleanup isolation valves are closed.

When the SLCS is initiated to inject a liquid neutron absorber into the reactor, the following devices are actuated:

(a) One of the two injection valves is opened.

(b) One of the two storage tank discharge valves is opened.

(c) One of the two injection pumps is started.

(d) The reactor water cleanup isolation valves are closed.

Additionally, the pressure and tank level sensing equipment indicates that the SLCS is pumping liquid into the reactor.

(10) Separation

The SLCS is separated both physically and electrically from the CRD System. The SLCS electrical control channels are separated in accordance with the requirements of Subsection 8.3.3.6.2

(11) Testability

The SLCS is capable of being tested by manual initiation of actuated devices during normal operation. In the test mode, demineralized water is circulated in the SLCS loops rather than sodium pentaborate. During reactor shutdown, demineralized water may be injected into the reactor vessel for the injection test mode.

(12) Environmental Considerations

The environmental considerations for the instrument and control portions of the SLCS are the same as for the active mechanical components of the system (Section 3.11).The instrument and control portions of the SLCS are seismically qualified not to fail during, and to remain functional following, a safe shutdown earthquake (SSE) (see Section 3.10 for seismic qualification aspects).

(13) Operational Considerations

The control scheme for the SLCS can be found in the interlock block diagram (Figure 7.4-1). The SLCS is automatically initiated upon receiving an ATWS signal or can be manually initiated in the control room by inserting the key in the A or B keylocking switch and turning it to the START position. It will take between 60 and 150 minutes to complete the injection and for the storage tank level sensors to indicate that the storage tank is dry (e.g., injection will occur in 61 minutes at minimum tank level with both pumps operating). When the injection is completed, the system automatically shuts down on low tank level or may be manually turned off by turning the keylocking switch counterclockwise to the STOP position.

(14) Reactor Operator Information

(a) The following items are located in the control room for operation information:

(i) Analog Indication

— Storage tank level

— System pressures

(ii) Status Lights

— Pump or storage tank outlet valve overload trip or power loss

— Position of injection line manual service valve

— Position of storage tank outlet valve and in-test status

— Position of test tank discharge manual service valve

— SLCS manually out of service

— Pump auto trip

(iii) Annunciators

The SLCS annunciators indicate:

— Manual or automatic out-of-service condition of SLCS A and/or B due to:

- Operation of manual out-of-service switch

- Storage tank outlet valve in test status

- Overload trip or power loss in pump or storage tank outlet valve controls

— Standby liquid storage tank high or low temperature

— Standby liquid tank high or low level

— Standby liquid pump A (B) auto trip

(b) The following items are located locally at the equipment for operator utilization:

(i) Analog Indication

— Storage tank level

— System pressures

— Storage tank temperature

(ii) Indicating lamps

— Pump status

— Storage tank operating heater status

— Storage tank mixing heater status

(15) Setpoints

The SLCS has setpoints for the various instruments as follows:

(a) The high and low standby liquid temperature switch is set to activate the annunciator at temperatures outside the range allowed for correct chemical balance of the boron concentration.

(b) The high and low standby liquid storage tank level switch is set to activate the annunciator when the level is outside its allowable limits.

(c) The low standby liquid storage tank level switches are set to trip the operating pumps when the level is low.

(d) The thermostatic controller and operating heater assure that the temperature of the liquid is maintained within the range allowed for correct chemical balance of the boron concentration.

The Technical Specifications for the SLCS are in Chapter 16.

7.4.1.3 Reactor Shutdown Cooling Mode–Instrumentation and Controls

(1) Function

The SDC mode of the RHR System is used during the normal or emergency reactor shutdown and cooldown. The RHR System P&ID is Figure 5.4-10 and the RHR System IBD is Figure 7.3-4.

The initial phase of the SDC mode is accomplished following insertion of the control rods and steam blowdown to the main condenser which serves as the heat sink.

Reactor shutdown cooling has three independent loops. Each loop consists of pump, valves, heat exchanger, and instrumentation designed to provide decay heat removal capability for the core. This mode specifically accomplishes the following:

(a) Reactor Shutdown–removes enough residual heat (decay and sensible) from the reactor vessel water to cool it to 60°C within 24 hours after the control rods are inserted, then maintains or reduces this temperature so that the reactor can be refueled and serviced. This mode is manually activated with the reactor pressure below 0.93 MPaG, with all three SDC loops available.

(b) Safe Shutdown (Emergency Shutdown) brings the reactor to a cold shutdown condition (< 100°C) within 36 hours after control rod insertion. This mode is manually activated with the reactor pressure below 0.93 MPaG, with two-out-of-three shutdown cooling loops available.

The RHR mode can accomplish its design objective by a preferred means by directly extracting reactor vessel water from the vessel shutdown nozzle and routing it to a heat exchanger and back to the vessel. Cooling water is returned to the vessel via the feedwater line (Loop A) and via the core cooling injection nozzles (Loops B and C).

(2) Classification

Electrical components for the reactor SDC mode of the RHR System are safety-related and are classified as Class 1E.

(3) Power Sources

This system utilizes normal plant power sources. These include 4.16 kV for the pumps, 480 VAC/120 VAC instrument buses, and as backed up by DC sources. If for any reason the normal plant sources become unavailable, the system is designed to utilize the emergency buses and sources.

(4) Equipment

The reactor water is cooled by taking suction from the three SDC suction nozzles. The water is pumped through the system heat exchanger and back to the reactor vessel via the feedwater lines (Loop A) and the LPFL injection nozzles (Loops B and C).

If it is necessary to discharge a complete core load of reactor fuel to the fuel pool, a means is provided for making a physical intertie between the Spent Fuel Pool Cooling and Cleanup (SFPC) System and the RHR heat exchangers. This increases the cooling capacity of the SFPC System to handle the heat load for this situation.

(5) Initiating Circuits

The reactor Shutdown Cooling System is initiated by manual operator actions.

(6) Logic and Sequencing

The following reactor shutdown cooling operating sequence is to be utilized:

(a) The RHR valving should be aligned for shutdown cooling mode.

(b) The RHR heat exchangers and service water are lined up for cooling.

(7) Bypasses and Interlocks

To prevent opening of the reactor shutdown cooling valves except under proper conditions, the interlocks are provided as shown in Table 7.4-1.

The three RHR pumps used for shutdown cooling are interlocked to trip if the reactor SDC valves and suction valves from the suppression pool are not properly positioned.

(8) Redundancy

The reactor SDC System contains three loops. Any two of the three loops is sufficient to satisfy the cooling requirements for emergency shutdown cooling. Each loop has its own suction line with three suction valves in series. In the event one of the suction valves fails closed, normal shutdown cooling is not available for that loop. The remaining two loops will provide the shutdown cooling.

Refer to Chapter 15 for a system-level examination of the above operation.

Although there is not an instrumentation diversity requirement for the reactor SDC System, the design basis objective is achieved by providing three independent SDC loops.

(9) Actuated Devices

All valves in the SDC mode are equipped with remote manual switches in the main control room. The only automatically activated modes of the RHR are the LPFL mode for the ECCS and the suppression pool cooling mode, as described in

Subsections 7.3.1.1.1.4 and 7.3.1.1.4, respectively. Other modes of RHR are described in Subsection 7.3.1.1.3.

(10) Separation

Since various modes of operation of the RHR System perform safety-related functions (LPFL suppression pool cooling and wetwell and drywell spray cooling), any of the system equipment performing safety-related functions satisfies the appropriate safety separation criteria. The SDC mode of operation can utilize two diverse techniques. Separation between components utilizes three completely independent loops and thus satisfies safety separation criteria in order to accomplish its design basis.

(11) Testability

The reactor SDC pumps (RHR) may be tested to full capacity during normal plant operation. All valves except those isolated by reactor pressure interlock in the system may be tested during normal plant operation from the remote manual switches in the main control room.

SSLC testing as discussed in Subsection 7.1.2.1.6, is also applicable here for the reactor SDC mode function of RHR System.

(12) Environmental Considerations

The only reactor SDC control component located inside the drywell that must remain functional in the environment is the control mechanism for the inboard isolation SDC valve. The control and instrumentation equipment located outside the drywell is selected in consideration of the normal and accident environments in which it must operate.

The RHR equipment is seismically qualified and environmentally classified as discussed in Sections 3.2, 3.10, and 3.11.

(13) Operational Considerations

All controls for reactor shutdown cooling are located in the main control room. Reactor operator information is provided as described in the RHR discussion of LPFL mode (Subsection 7.3.1.1.1.4).

(14) Setpoints

There are no setpoints involved in the operation of the SDC mode of the RHR System except that reactor pressure and water level setpoints must be satisfied before the operator can begin this mode.

7.4.1.4 Remote Shutdown System

7.4.1.4.1 General

The Remote Shutdown System (RSS) provides a means to carry out the reactor shutdown functions from outside the main control room and bring the reactor to hot shutdown and subsequent cold shutdown through suitable procedures, in a safe and orderly fashion. The RSS instrument electrical diagram (IED) is provided as Figure 7.4-2. The RSS interlock block diagram (IBD) is provided as Figure 7.4-3.

7.4.1.4.2 Postulated Conditions Assumed to Exist as the Main Control Room Becomes Inaccessible

(1) The plant is operating initially at or less than design power.

(2) The plant is not experiencing any transient situations. Even though the loss of offsite AC power is considered unlikely, the remote shutdown panel or facilities are powered from the Class 1E power system so that backup AC power would be automatically supplied by the plant diesel generator. Manual controls of the diesel generator are also available locally.

(3) The plant is not experiencing any accident situations. No design basis accident (including a LOCA) shall be assumed, so that complete control of engineered safeguard feature systems from outside the main control room shall not be required.

(4) All plant personnel have evacuated the main control room.

(5) The main control room continues to be inaccessible for several hours.

(6) The initial event that causes the main control room to become inaccessible is assumed to be such that the reactor operator can manually scram the reactor before leaving the main control room. If this was not possible, the capability of opening the RPS logic input power breakers from outside the main control room can be used as a backup means to achieve initial reactor reactivity shutdown.

(7) The main turbine pressure regulators may be controlling reactor pressure via the bypass valves. However, in the interest of demonstrating that the plant can accommodate even the loss of the turbine controls, it is assumed that this turbine generator control panel function is also lost. Therefore, main steamline isolation is assumed to occur at a specified low turbine inlet pressure and reactor pressure is relieved through the relief valves to the suppression pool.

(8) The reactor Feedwater System, which is normally available, is also assumed to be inoperable. Reactor water is made up by the HPCF System.

(9) It shall be assumed that the event causing the evacuation will not cause any failure of the DC or AC control power supplies to the remote shutdown panels or any failure of the DC or AC power feeds to the equipment whose functions are being controlled from the remote shutdown panels.

The above initial conditions and associated assumptions are very severe and conservatively bound any similar postulated situation.

7.4.1.4.3 Remote Shutdown Capability Description

(1) The capability described provides remote control for reactor systems needed to carry out the shutdown function from outside the main control room and bring the reactor to hot shutdown and subsequent cold shutdown through suitable procedures.

(2) It provides a variation to the normal system used in the main control room permitting the shutdown of the reactor when feedwater is unavailable and the normal heat sinks (turbine and condenser) are lost.

(3) Reactor pressure will be controlled and core decay and sensible heat rejected to the suppression pool by relieving steam pressure through the automatic activation of relief valves. Reactor water inventory will be maintained by the HPCF System. During this phase of shutdown, the suppression pool will be cooled by operating the RHR System in the SPC mode.

(4) Manual operation of the relief valves will cool the reactor and reduce its pressure at a controlled rate until reactor pressure becomes so low that HPCF System operation is discontinued.

(5) The RHR System will then be operated in the SDC mode using the RHR System heat exchanger in the reactor water circuit to bring the reactor to the cold low pressure condition.

7.4.1.4.4 Remote Shutdown Capability Controls and Instrumentation–Equipment, Panels, and Displays

(1) **Main Control Room**–Remote Shutdown Capability Interconnection Design Considerations

Some of the existing systems used for normal reactor shutdown operations are also utilized in the remote shutdown capability to shut down the reactor from outside the main control room. The functions needed for remote shutdown control are provided with manual transfer devices which override controls from the main control room and transfer the controls to the remote shutdown control. Control signals are interrupted by the transfer devices at the hardwired, analog loop. Process signals to the main control room are routed from the sensor, through the transfer devices on the remote shutdown panels, and then to the Remote Digital Logic Controllers (RDLCs) for use in the main control room. Similarly, control signals from the main control room are routed from the RDLCs, through the remote shutdown transfer devices, and then to the interfacing system equipment. Actuation of the transfer devices interrupts the connection to the RDLCs and transfers control to the Remote Shutdown System. Control of all necessary power supply circuits are also transferred to the remote shutdown system. Remote shutdown control is not possible without actuation of the transfer devices. Operation of the transfer devices causes an alarm in the main control room. The remote shutdown control panels are located outside the main control room. Access to this point is administratively and procedurally controlled.

Instrumentation and controls located on the remote shutdown control panels are shown in instrument and electrical diagram Figure 7.4-2.

(2) High Pressure Core Flooder (HPCF)

(a) The following HPCF System loop B equipment functions have transfer and control switches located on the Division II remote shutdown control panel:

(i) Valve (pump suction from condensate storage)

(ii) Valve (HPCF injection)

(iii) Valve (minimum flow to suppression pool)

(iv) Valve (test line isolation)

(v) Valve (pump suction from suppression pool)

(vi) HPCF Pump (B)

(see HPCF P&ID in Section 6.3)

(b) The following HPCF System instrumentation is provided on the Division II remote shutdown control panel:

(i) HPCF flow indication

(ii) HPCF pump discharge pressure indication

(iii) Indicating lights for all valve (with RSS interface) positions and for the HPCF pump B stop/run

(3) Residual Heat Removal (RHR) System

(a) The following RHR System equipment functions have transfer and control switches located on one or both remote shutdown panels as indicated:

(i) Residual heat removal pump A, B
(ii) Valve (suppression pool suction) A, B
(iii) Valve (heat exchanger bypass) A, B
(iv) Valve (shutdown cooling injection) A, B
(v) Valve (heat exchanger outlet) A, B
(vi) Valve (suppression pool injection) A, B
(vii) Valve (shutdown cooling suction - inboard isolation) A, B
(viii) Valve (shutdown cooling suction - outboard isolation) A, B
(ix) Valve (shutdown cooling suction) A, B
(x) Valve (minimum flow) A, B
(xi) Valve (liquid waste flush isolation) A, B
(xii) Valve (drywell spray) B
(xiii) Valve (wetwell spray) B
(xiv) Valve (fuel pool cooling isolation) B

(b) The following RHR instrumentation is located on both remote shutdown control panels as indicated:

(i) RHR flow indication (A,B)
(ii) RHR heat exchanger inlet temperature indication (A,B)
(iii) RHR heat exchanger outlet temperature indicators (A,B)
(iv) RHR heat exchanger bypass valve position (A,B)
(v) RHR heat exchanger outlet valve position (A,B)
(vi) RHR pump discharge pressure indication (A,B)
(vii) Indicating lights for valve (with RSS interface) positions and for RHR pump stop/run (A,B)

(4) Nuclear Boiler System

(a) The following functions have transfer and control switches located at the remote shutdown control panels:

Four air-operated safety relief valves (SRVs) (The valves are 125 VDC solenoid pilot operated.). Three of these valves have switches on the Division I panel, the fourth valve has switches on the Division II panel.

(b) The following nuclear boiler instrumentation is provided on the remote shutdown control panels as indicated:

(i) Reactor water level wide range indication (A,B)

(ii) Reactor water level shutdown range indication (A,B)

(iii) Reactor pressure indication (A,B)

(iv) Indicate lights for four SRV valve open/close condition (three on Panel A, and one on Panel B

(5) Reactor Building Cooling Water (RCW) System

(a) The following functions have transfer and control switches located on the remote shutdown panels as indicated:

(i) RCW pumps (A,D and B,E)

(ii) RCW heat exchanger cooling water outlet valves (A,D,G and B,E,H)

(iii) RCW, RHR heat exchanger, outlet valve (A,B)

(iv) RCW, diesel generator, outlet valve (A,D and B,E)

(v) RCW separator valve between essential and non-essential loads (A,B)

(vi) RCW temperature control valves (A,B)

(b) The following RCW instrumentation is provided on the RSS control panels as indicated:

(i) RCW loop flow indication (A,B)

(ii) Indicating lights for valve positions and for pump stop/run (A,B)

(6) Reactor Service Water System (RSW)

(a) The following functions have transfer and control switches located on the remote shutdown panels as indicated:

(i) RSW Pumps (A,D and B,E)

(ii) RCW heat exchanger service water inlet valve (A,D,G and B,E,H)

(iii) Service water strainer outlet valve (A,D and B,E)

(iv) Service water strainer inlet valve (A,D and B,E)

(v) RCW heat exchanger service water outlet valve (A,D,G and B,E,H)

(vi) Service water strainer flush valve (A,D and B,E)

(vii) Service water supply valve (A,B)

(viii) Service water return valve (A, B)

(b) The following RSW instrumentation is provided on the RSS control panels as indicated:

(i) Indication of differential pressure between inlet and outlet of service water strainers (A,D and B, E)

(ii) Indicating lights for all valve positions and RSW pump stop/run conditions are provided on both RSS panels.

(7) Electrical Power Distribution System (EPDS)

(a) The following functions have transfer and control switches located on the Division I remote shutdown panel:

(i) Safety Bus A3 Breaker from UAT A

(ii) Safety Bus A3 Breaker from RAT A

(iii) Safety Bus A3 Breaker from Emergency Diesel Generator A

(iv) Safety Bus A3 Breaker from Bus CTG3

(v) Safety Bus A3 Breaker to P/C E20

(vi) 480V feeder breaker: TR to P/C E20

(b) The following functions have transfer and control switches located on the Division II remote shutdown panel:

(i) Safety Bus B3 Breaker from UAT B

(ii) Safety Bus B3 Breaker from RAT A

(iii) Safety Bus B3 Breaker from Emergency Diesel Generator B

(iv) Safety Bus B3 Breaker from Bus CTG3

(v) Safety Bus B3 Breaker to P/C F20

(vi) 480V feeder breaker: TR to P/C F20

(c) A 4160V voltmeter is provided on RSS panels A,B, respectively.

(8) Not Used

(9) Atmospheric Control (AC) System

(a) Suppression pool level indication is provided on both RS panels.

(10) Makeup Water Condensate System (MUWC)

(a) Condensate storage pool level indication is provided on RS panel B.

(11) Suppression Pool Temperature Monitoring System (SPTM)

(a) Suppression pool temperature indication is provided on both RS panels.

(12) Emergency Diesel Generator (DG) System

(a) A transfer switch on each RS panel (A,B) permits DG control (start/stop) from the control room to be interrupted. There are no DG controls on the RS panels. During remote shutdown operation, the DGs can be controlled locally.

(b) Status lights provide DG status indication (run/stop) on each RS panel (A,B).

7.4.2 Analysis

7.4.2.1 Alternate Rod Insertion Function

7.4.2.1.1 General Functional Requirements Conformance

The Recirculation Flow Control System (RFCS) includes the logic for both automatic initiation and manual initiation of the ARI function. When the RFCS initiates the ARI function, related ARI activation signals are provided to the ARI valves of the CRD system and to the Rod Control and Information System for activation of the ARI motor run-in function.

Upon initiation of the ARI function, the RFCS logic assures that the activation signals for the ARI valves will remain continuously energized sufficiently long to assure that the time-delayed, rapid hydraulic insertion of the control rods will occur by depressurizing the scram valves of the CRD hydraulic control units. This provides for a diverse means of hydraulic insertion of the control rods from the normal Reactor Protection System (RPS) initiated scram hydraulic insertion function.

The alternate rod insertion (ARI) motor run-in function is accomplished by the Rod Control and Information System (RCIS) and the Fine-Motion Control Rod Drive (FMCRD) Subsystem. This function provides an alternate method of driving control rods into the core which is diverse from the hydraulic insertion functions.

The RFCS, the ARI valves, and the FMCRD components associated with the motor run-in function of the CRD System, and the RCIS are not required for safety, nor are these components qualified in accordance with safety-related criteria. However, the FMCRD components associated with hydraulic scram are qualified in accordance with safety criteria.

The subsystem's inherent diversity provides mitigation of the consequences of (ATWS) anticipated transient without scram events. This capability is discussed in Subsection 7.7.1.2.2.

The ARI design is in full compliance with the design considerations cited in NEDE-31096-P-A (Reference 7.4-1).

7.4.2.1.2 Specific Regulatory Requirements Conformance

Table 7.1-2 identifies the ARI function and the associated codes and standards applied. In addition to GDCs 13 and 19 (applied to non-safety-related system/ functions in accordance with the SRP, Section 7.7), GDC 25 and Reg. Guide 1.75 are also addressed relative to the shutdown characteristics of the subsystem and its interface with the essential power buses. 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)

Although the ARI is not Class 1E, the portions of the FMCRD used for the hydraulic scram function are qualified as Class 1E. These functions are analyzed along with the Reactor Protection System (trip) discussed in Section 7.2.

With regard to IEEE-603, Section 5.6.3, signals from safety system equipment that interface with the non-safety system equipment that implements the ARI function (e.g., the low reactor water level status signals provided to the RFCS) are optically isolated so that failure of the non-safety equipment that implements the ARI function cannot affect any safety-related function.

The RCIS logic has been designed such that the only single failure that may result in insertion failure of that rod when the ARI function is activated is the failure of the logic and individual local control equipment (e.g., stepping motor driver module or rod brake controller) associated with FMCRD motor movement of one control rod. Also, two manual actions are required at the Main Control Room Panel to manually initiate ARI.

(2) General Design Criteria (GDC)

(a) **Criteria:** GDCs 13, 19, and 25.

(b) **Conformance:** The ARI is in compliance (in part, or as a whole, as applicable) with these GDCs. All GDCs are generically addressed in Subsection 3.1.2.

(3) Regulatory Guides (RGs)

(a) RG 1.75–"Physical Independence of Electric Systems"

The ARI is not required for safety, nor are its components considered Class 1E. The subsystem derives control power from the non-1E UPS buses. However, for ATWS considerations, the reliability of the subsystem is enhanced by using Class 1E power for the drive motors.

There are three separate groups of non-1E drives with each receiving power from Division I Class 1E bus. Class 1E circuit breakers are used as isolation devices in accordance with IEEE-384. The breakers are designed to trip on fault current only and are not tripped for LOCA.

A LOCA trip of these breakers could preclude the advantages of ARI for postulated ATWS conditions.

The circuit protection coordination and testing of breakers assures that the FMCRDs breaker time-over-current trip characteristic for all circuit faults shall cause the breaker to interrupt the fault current prior to trip initiation of any upstream breaker. The power source shall supply the necessary fault current for sufficient time to ensure the proper coordination without loss of function of Class 1E loads.

In addition, each FMCRD inverter has current limiting features to limit the FMCRD motor fault current. Refer to Subsection 8.3.1.1.1 for additional description of design features incorporated for preventing degradation of operation of any Class 1E loads if a fault condition exists in the non-Class 1E equipment that provides power for the FMCRD motors.

7.4.2.2 Standby Liquid Control System (SLCS) — Instrumentation and Controls

7.4.2.2.1 General Functional Requirements Conformance

Redundant positive displacement pumps, injection valves, storage tank outlet valves, and control circuits (Subsection 7.4.1.2) constitute all of the active equipment required for injection of the sodium pentaborate solution. Indicator lights provide indication on the reactor control bench board of system status. Testability and redundant power sources are described in this subsection and Subsection 7.4.1.2.

Chapter 15 examines the system-level aspects of the SLCS under applicable plant events. Loss of plant instrument air or cooling water will not, by itself, prevent this reactor shutdown capability.

7.4.2.2.2 Specific Regulatory Requirements Conformance

Table 7.1-2 identifies the Standby Liquid Control System (SLCS) 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 SLCS is manually actuated (or automatically actuated for ATWS events) and serves as a backup method for shutting down the reactor when no control rods can be inserted from the full power setting. It is not necessary for the SLCS to meet the single-failure criterion because it is considered redundant to (and therefore kept independent of) the control rod scram system.

There are two channels of control circuits, discharge pumps and motors, storage tank discharge valves and injection valves. These two channels are independent of each other so that failure in one channel will not prevent the other from operating. No components of the SLCS are required to operate in the drywell environment. An isolation check valve is the only component located inside the drywell. Other SLCS equipment are designed to remain functional following an SSE.

The SLCS design is similar to the GESSAR II design, except the explosive (squib) injection valves are replaced with motor-operated injection valves. It is designed to meet all applicable portions of IEEE-603 as clarified above.

(2) General Design Criteria (GDCs)

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

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

(b) **Conformance:** The SLCS is in compliance (in part, or as a whole, as applicable) with these GDCs. All GDCs are generically 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 SLCS:

(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 Issues”

(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”

As indicated in Paragraph (1), the SLCS is not required to meet the single-failure criterion (RG 1.53) since it is designed to be redundant (and diverse) from the control rod scram system. However, the two channels of active components assure that no single failure of these components will prevent the SLCS from accomplishing its boron injection function. Passive components which are not redundant include the boron tank, injection pipeline, etc.

With that clarification, the SLCS (in combination with the rod scram system) fully meets the intent of the Regulatory Guides listed above.

(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 SLCS. 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 SLCS is in full compliance with this BTP.

(b) BTP ICSB 22– “Guidance for Application of Regulatory Guide 1.22” All actuated equipment within the SLCS can be tested during reactor operation. Actual injection can be simulated during shutdown using demineralized water.

(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 SLCS.

7.4.2.3 Reactor Shutdown Cooling Mode — Instrumentation and Controls

7.4.2.3.1 General Functional Requirements Conformance

The design of the reactor shutdown cooling mode of the RHR System meets the general functional requirements as follows:

(1) Valves

Manual control and position indication is provided in the main control room. Three independent loops assure that no single failure in the valve electrical circuitry can result in loss of capability to perform a safety function.

Interlocks are provided to close the valves if a low reactor water level signal is present or if high reactor pressure exists.

(2) Instrumentation

Indicators are provided for RHR pump inlet and discharge pressures, heat exchanger outlet flow, discharge line level, and heat exchanger inlet and discharge temperatures.

(3) Alarms

The following system functional alarms apply to all modes of the RHR System and to each of the three RHR loops except as noted:

(a) Motor overload of any pump.

(b) Heat exchanger service water outlet temperature high.

(c) High wetwell air space temperature.

(d) Low reactor pressure.

(e) Discharge line pressure too high or too low.

(f) ELCS Out of Service.

(g) Suppression pool temperature high (common alarm).

(h) Shutdown line pressure high.

(i) Level 1 water level (common alarm).

(j) High drywell pressure (common alarm).

(k) Overload of any RHR valve.

(l) LPFL Manual initiation armed.

(m) RHR autostart.

(n) Loop out of service.

(o) RHR MOVs in test status.

(p) Pump motor auto trip.

(q) Fill pump trip.

(r) Pump operation switch in pull-lock.

(s) Pump suction valve closed.

(4) Pumps

Manual controls and stop and start indicators are provided in the control room. Interlocks are provided to trip the pumps if the shutdown suction valves are not open and no other suction path exists.

Chapter 15 considers the operation and the system-level qualitative aspects of this system.

Loss of plant instrument air will not, by itself, prevent reactor shutdown capability.

7.4.2.3.2 Specific Regulatory Requirements Conformance

Table 7.1-2 identifies the RHR SDC mode with 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 SDC mode of the RHR System is a three-loop, three-division system which is redundantly designed so the failure of any single element will not interfere with the required safety action of the system. As an operating mode of the RHR System, the system is designed to meet the same requirement as the ECCS.

All components used for the safety isolation functions are qualified for the environments in which they are located (Sections 3.10 and 3.11). However, this mode of the RHR System (unlike the LPFL mode which is automatically actuated by LOCA) is manually actuated providing reactor pressure and water level are at permissible levels.

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 SC 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 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.

Those portions of IEEE-603 which relate to automatically initiated systems are not applicable to the manually actuated shutdown cooling mode of the RHR System. However, the system is designed in accordance with all other requirements of IEEE-603 as described in Subsection 7.4.1.3.

(2) General Design Criteria (GDC)

In accordance with the Standard Review Plan for Section 7.4 and with Table 7.1-2, with the following GDCs are addressed for the SCM:

(a) **Criteria:** GDCs 13, 15, 19, 34, and 44.

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

(3) Regulatory Guides (RGs)

In accordance with the Standard Review Plan for Section 7.4, and with Table 7.1-2, the following RGs are addressed for the SCM:

(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 SCM 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.

With regard to RG 1.105, there are no actuation setpoints, since the SC mode is manually initiated. However, reactor pressure and level interlocks are provided to assure the mode cannot be actuated under the wrong conditions. These interlocks are derived from shared signals in the Nuclear Boiler System.

(4) Branch Technical Positions (BTPs)

In accordance with the Standard Review Plan for Section 7.4, and with Table 7.1-2, the following BTPs are addressed for the SCM:

(a) BTP ICSB 3– "Isolation of Low Pressure Systems from the High Pressure Reactor Coolant System"
The SDC mode of the RHR System has both inboard and outboard HP/LP isolation valves on both the suction and injection ends of the system. The injection end is the same as the LPFL mode and meets the requirements of B.3 as discussed in Paragraph (4a) of Subsection 7.3.2.1.2.

The three separate SCM suction lines each have motor-operated HP/LP isolation valves on both the inboard and outboard sides of the drywell wall.

There are four sensors (originating from the NBS and shared with other systems) which monitor reactor pressure and are combined in two-out-of-four

* See Subsection 7.1.2.10.9.

logic to provide the high reactor pressure interlock signal. Reactor water Level 3 is also monitored in similar fashion to produce the low reactor level interlock signal. These two sets of two-out-of-four signals are combined in "OR" combination to close each valve (Figure 7.3-4). Each loop also has a separate signal to isolate on RHR equipment area ambient high temperature.

The inboard valves receive their interlock signals from Divisions I, II, and III, while the corresponding outboard valves receive their interlock signals from Divisions II, III, and I, respectively.

Thus, independence and diversity are utilized in the design in accordance with measure B.2 of 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.

(c) BTP ICSB 22– "Guidance for Application of Regulatory Guide 1.22"
In accordance with BTP ICSB 3, the suction and injection valves for the SC mode cannot be opened during reactor operating pressure. However, they can be routinely tested when the reactor is shut down. All other system components can be tested during normal operation in accordance with this BTP.

(5) TMI Action Plan Requirements (TMI)

In accordance with the Standard Review Plan for Section 7.4, and with Table 7.1-2, there are no TMI action plan requirements applicable to the SCM.

7.4.2.4 Remote Shutdown System–Instrumentation and Controls

7.4.2.4.1 General Functional Requirements Conformance

The Remote Shutdown System (RSS) is classified as a safety-related system because it interfaces with nuclear safety-related equipment in other systems. No LOCA, seismic event or other abnormal plant condition (except loss of offsite power) is assumed to occur coincident with the event necessitating control room evacuation. It is assumed that the emergency AC power buses are energized by normal AC power (offsite power) or by the backup diesel generators.

The RSS provides instrumentation and controls outside the main control room to allow prompt hot shutdown of the reactor after a scram and to maintain safe conditions during hot shutdown. It also provides capability for subsequent cold shutdown of the reactor through the use of suitable procedures.

7.4.2.4.2 Specific Regulatory Requirements Conformance

Table 7.1-2 identifies the Remote Shutdown System (RSS) 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 Remote Shutdown System (RSS) consists of two panels (Division I and Division II) which are located in separate rooms in the Reactor Building.

The RSS provides remote control capability as defined by the following interfaces:

System	Total Channels	RSS Interface
Residual Heat Removal	A, B, C	A, B
High Pressure Core Flooder	B, C	B
Nuclear Boiler System	A, B, C, D	A, B
Reactor Bldg. Cooling Water	A, B, C	A, B
Reactor Service Water	A, B, C	A, B
Electrical Power Distribution	I, II, III, IV	I, II

The RSS is designed such that it does not degrade the capability of the interfacing systems. All equipment is qualified as Class 1E, consistent with the safety-related interfaces.

Separation and isolation is preserved both mechanically and electrically in accordance with IEEE-603 and Regulatory Guide 1.75.

With regard to Paragraph 5.1 of IEEE-603, a single-failure event is assumed to have occurred to cause the evacuation of the control room. The RSS is not designed to accommodate additional failures for all scenarios. The effects of such failures are analyzed as follows:

The loss of one complete RHR loop could extend the time needed for the reactor to reach the emergency shutdown conditions. However, the ability of the RSS to ultimately facilitate such conditions is not impaired. An analysis was performed for this scenario using the nominal decay heat curve. The results showed that the time to reach 100°C with only one RHR loop available varied from 38 to 51.4 hours as the temperature of the ultimate heat sink varied from 29 to 35°C.

In the event of a complete loss of Division II, safe shutdown can be achieved by depressurizing the reactor with the three SRVs in Division I to the point at which RHR shutdown cooling can be initiated. This assumes that the operator reaches the RSS panels in a timely manner (i.e., within 10 minutes after scram). No core uncovering is expected even though no high pressure coolant makeup capability is available.

In the event of a complete loss of Division I, the reactor can be depressurized with one SRV in Division II. Therefore, the time required to reach low pressure conditions will be extended. However, the probability of an event requiring control room evacuation in addition to a failure resulting in loss of Division I (external to the control room) is so low that it is not considered credible.

Other sections of IEEE-603 which relate to testability of sensors, etc., are not applicable to the RSS of itself, but are applicable to the primary systems which interface with the RSS. All other applicable criteria of IEEE-603 are met by the RSS.

(2) General Design Criteria (GDC)

In accordance with the Standard Review Plan for Section 7.4, and with Table 7.1-2, the following GDCs are addressed for the RSS:

(a) **Criteria:** GDCs 2, 4, 13, 19, 33, 34, 35, and 44.

(b) **Conformance:** Assuming the clarification for a single failure explained in Subsection (1) above, the RSS is in compliance (in part, or as a whole, as applicable) with the GDCs identified in (a). All GDCs are generically discussed in Subsection 3.1.2.

(3) Regulatory Guides (RGs)

In accordance with the Standard Review Plan for Section 7.4, and with Table 7.1-2, the following Reg. Guides are addressed for the RSS:

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

(b) RG 1.62– “Manual Initiation of Protection Actions”

(c) RG 1.75– “Physical Independence of Electric Systems”

With regard to Regulatory Guide 1.53, a single failure is assumed to have occurred which caused the need to evacuate the control room. The RSS is not designed to accommodate an additional failure for all scenarios. The result of postulated worst case additional failures is discussed in (1) above. Otherwise, the RSS conforms with the above listed Reg. Guides assuming the same interpretations and clarifications identified in Subsections 7.3.2.1.1 and 7.1.2.10.

(4) Branch Technical Positions (BTPs)

In accordance with the Standard Review Plan for Section 7.4, and with Table 7.1-2, there are no BTPs applicable for the RSS.

(5) TMI Action Plan Requirements (TMI)

In accordance with the Standard Review Plan for Section 7.4 and with Table 7.1-2, there are no TMIs applicable for the RSS. However, all TMI action plan requirements are generically addressed in Appendix 1A.

7.4.3 References

7.4-1 NEDE-31096-P-A, L. B. Claassen, et. al., "Anticipated Transients Without Scram Response to NRC ATWS Rule", 10 CFR 50.62, February 1987.

Table 7.4-1 Reactor Shutdown Cooling Bypasses and Interlocks

Valve Function	Reactor Pressure Exceeds Shutdown Cooling Permissive	Isolation Valve Closure Signal
Inboard suction isolation*	Cannot open	Closes (A)†
Outboard suction isolation*	Cannot open	Closes (A)
Reactor injection‡	Cannot open*ƒ*	Closes (A)
Radwaste discharge inboard*	Can open (M)**	Closes (M)
Radwaste discharge outboard*	Can open (M)	Closes (M)
Valve function††		
Inboard suction isolation	Closes (A)*ƒ*	Closes (A)
Outboard suction isolation	Closes (A)	Closes (A)
Reactor injection	Closes (A) *ƒ*	Closes (A)

* Valves have manual control for opening.

† (A) denotes automatic.

‡ Valves have manual and auto control for opening.

ƒ Injection valve cannot be opened at reactor pressure above the injection pressure (approx. 3.04 MPa G).

** (M) denotes manual.

†† Valves have manual and auto control for closing; manual close is not constrained.

The following figures are located in Chapter 21: