# Chapter 7
# Table of Contents

# Chapter 7
# List of Tables

# Chapter 7
# List of Figures

# List of Figures (Continued)

# List of Figures (Continued)

# 7.0 Instrumentation and Control Systems

## 7.1 Introduction

This chapter presents the specific detailed design and performance information relative to the instrumentation and control (I&C) aspects of the safety-related systems utilized throughout the plant. The design and performance considerations relative to these systems' safety function and their mechanical aspects are described in other chapters.

### 7.1.1 Identification of Safety-Related Systems

#### 7.1.1.1 General

Instrumentation and control systems are designated as either non-safety-related systems or safety systems, depending on their function. Some portions of a system may have a safety function, while other portions of the same system may be classified non-safety-related. A description of the system of classification can be found in Chapter 15, Appendix A.

The systems presented in Chapter 7 are also classified according to NRC Regulatory Guide 1.70,(i.e., reactor protection (trip) system (RPS), engineered safety feature (ESF) systems, systems required for safe shutdown, safety-related display instrumentation, all other instrumentation systems required for safety, and control systems not required for safety). Table 7.1-1 compares I&C systems of the ABWR with those of the GESSAR II 238 Nuclear Island. Differences and their effect on safety-related systems are also identified in Table 7.1-1.

Each individual safety-related system utilizes redundant channels of safety-related instruments for initiating safety action. The automatic decision making and trip logic functions associated with the safety action of several safety-related nuclear steam supply systems (NSSS) are accomplished by a four-division correlated and separated protection logic complex called the safety system logic and control (SSLC). The SSLC multi-divisional complex includes divisionally separate control room and other panels which house the SSLC equipment for controlling the various safety function actuation devices. The SSLC receives input signals from the redundant channels of instrumentation in the safety-related system, and uses the input information to perform logic functions in making decisions for safety actions.

Divisional separation is also applied to the essential multiplexing system (EMS), which provides data highways for the sensor input to the logic units and for the logic output to the system actuators (actuated devices such as pump motors and motor-operated valves). Systems which utilize the SSLC are: (1) Reactor Protection (trip) System; (2) High Pressure Core Flooder System; (3) Residual Heat Removal System; (4) Automatic Depressurization System; (5) Leak Detection and Isolation System; (6) Suppression Pool Monitoring System; and (7) Reactor Core Isolation Cooling

System. The equipment arrangement for these systems and other supporting systems is shown in Figure 7.1-2.

### 7.1.1.2 Reactor Protection (Trip) System (RPS)

The Reactor Protection (trip) System instrumentation and controls initiate an automatic reactor shutdown via insertion of control rods (scram) if monitored system variables exceed preestablished limits. This action avoids fuel damage, limits system pressure and thus restricts the release of radioactive material.

[*The RPS and ESF (Subsection 7.1.1.3) Systems can be tested during reactor operation. Subsection 7.1.2.1.6 identifies testing, which, if, changed, requires NRC Staff review and approval prior to implementation. The applicable portions for this restriction are shown on Subsection 7.1.2.1.6 itself.* ]*

### 7.1.1.3 Engineered Safety Features (ESF) Systems

#### 7.1.1.3.1 Emergency Core Cooling Systems (ECCS)

Instrumentation and controls provide automatic initiation and control of specific core cooling systems such as High Pressure Core Flooder (HPCF) System, Automatic Depressurization System (ADS), Reactor Core Isolation Cooling(RCIC) System and the Low Pressure Flooder mode of the Residual Heat Removal (RHR) System provided to cool the core fuel cladding following a design basis accident.

#### 7.1.1.3.2 Leak Detection and Isolation System

Instrumentation and controls monitor selected potential sources of steam and water leakage or other conditions and automatically initiate closure of various isolation valves if monitored system variables exceed preestablished limits. This action limits the loss of coolant from the reactor coolant pressure boundary (RCPB) and the release of radioactive materials from either the RCPB or from the fuel and equipment storage pools.

#### 7.1.1.3.3 Wetwell and Drywell Spray Mode of RHR

Instrumentation and controls provide manual initiation of wetwell spray and drywell spray (when high drywell pressure signal is present) to condense steam in the containment and remove heat from the containment. The drywell spray has an interlock such that drywell spray is possible only in the presence of a high drywell pressure condition.

* See Section 3.5 of DCD/Introduction.

#### 7.1.1.3.4 Suppression Pool Cooling Mode of RHR (SPC-RHR)

Instrumentation and controls are provided to automatically or manually initiate portions of the RHR System to effect cooling of the suppression pool water.

#### 7.1.1.3.5 Standby Gas Treatment System

Instrumentation and control is provided to maintain negative pressure in the secondary containment and automatically limit airborne radioactivity release from the containment if required.

#### 7.1.1.3.6 Emergency Diesel Generator Support Systems

Instrumentation and control is provided to assure availability of electric control and motive power under all design basis conditions(DBAs). The function of the diesel generator is to provide automatic emergency AC power supply for the safety-related loads (required for the safe shutdown of the reactor) when the offsite source of power is not available.

#### 7.1.1.3.7 Reactor Building Cooling Water System

Instrumentation and control is provided to assure availability of cooling water for heat removal from the nuclear system as required. Safety-related portions of this system start automatically on receipt of a LOCA and/or LOPP (loss of preferred power) signal.

#### 7.1.1.3.8 Essential HVAC Systems

Instrumentation and control is provided to automatically maintain an acceptable thermal environment for safety equipment and operating personnel.

#### 7.1.1.3.9 HVAC Emergency Cooling Water System

Automatic instrumentation and control is provided to assure that adequate cooling is provided for the main control room, the control building essential electrical equipment rooms, and the diesel generator cooling coils.

#### 7.1.1.3.10 High Pressure Nitrogen Gas Supply System

Automatic instrumentation and control is provided to assure that adequate instrument high pressure nitrogen is available for ESF equipment operational support.

### 7.1.1.4 Safe Shutdown Systems

#### 7.1.1.4.1 Alternate Rod Insertion Function (ARI)

Though not required for safety, instrumentation and controls for the ARI provide a means to mitigate the consequences of anticipated transient without scram (ATWS) events. Upon receipt of an initiation signal (based on either high reactor dome pressure

or low reactor water level from the Recirculation Flow Control System), the RCIS System controls the fine motion control rod drive (FMCRD) motors such that all operable control rods are driven to their full-in position. This provides a method, diverse from the hydraulic control units (HCUs), for scramming the reactor.

#### 7.1.1.4.2 Standby Liquid Control System (SLCS)

Instrumentation and controls are provided for the manual initiation of an independent backup system (SLCS) which can shut the reactor down from rated power to the cold condition in the event that all withdrawn control rods cannot be inserted to achieve reactor shutdown. In addition, should the FMCRD fail to shut down the reactor during an ATWS event as described in Subsection 7.1.1.4.1, then instrumentation and controls are provided for the automatic initiation of SLCS.

#### 7.1.1.4.3 Residual Heat Removal (RHR) System/Shutdown Cooling Mode

Instrumentation and controls provide manual initiation of cooling systems to remove the decay and sensible heat from the reactor vessel.

#### 7.1.1.4.4 Remote Shutdown System

Manual instrumentation and controls are provided outside the main control room to assure safe shutdown of the reactor in the event that the main control room should become uninhabitable.

### 7.1.1.5 Safety-Related Display Instrumentation

Safety-related display instrumentation is provided to inform the reactor operator of plant conditions and equipment status so that it can be determined when a manual safety action should be taken or is required.

### 7.1.1.6 Other Safety-Related Systems

#### 7.1.1.6.1 Neutron Monitoring System (NMS)

The Neutron Monitoring System (NMS) monitors the core neutron flux from the startup source range to beyond rated power. The NMS provides logic signals to the Reactor Protection System (RPS) to automatically shut down the reactor when a condition necessitating a reactor scram is detected. The NMS is composed of the following subsystems:

(1) Startup Range Neutron Monitoring (SRNM)

(2) Local Power Range Monitoring (LPRM)

(3) Average Power Range Monitoring (APRM)

(4) Automated Traversing Incore Probe (ATIP)

(5) Multi-channel Rod Block Monitoring (MRBM)

#### 7.1.1.6.2 Process Radiation Monitoring System (PRMS) Instrumentation and Controls

The Process Radiation Monitoring System (PRMS) monitors the main steamlines, vent discharges and all liquid and gaseous effluent streams which may contain radioactive materials. Main control room display, recording and alarm capability is provided along with automatic trip inputs that initiate protection functions.

#### 7.1.1.6.3 High Pressure/Low Pressure Systems Interlock Protection Function

Instrumentation and controls provide automatic control of the RHR/LPFL System valves, thereby providing an interface between this low-pressure system and the reactor coolant pressure boundary to protect it from overpressurization.

#### 7.1.1.6.4 Deleted

#### 7.1.1.6.5 Wetwell-to-Drywell Vacuum Breaker System

This system is provided to automatically prevent the occurrence of undesirable negative pressure differential on the containment shell liner (see Subsection 6.2.1.1.4).

#### 7.1.1.6.6 Containment Atmospheric Monitoring System

The Containment Atmospheric Monitoring System (CAMS) measures and records radiation levels and the oxygen/hydrogen concentration in the primary containment under post-accident conditions. It is designed to operate continuously and is automatically put in service upon detection of LOCA conditions.

#### 7.1.1.6.7 Suppression Pool Temperature Monitoring System

Instrumentation is provided for automatic reactor scram and automatic suppression pool cooling initiation. Visual indications for operator awareness of pool temperature under all operating and accident conditions is also provided. The SPTM system is automatically initiated and continuously monitors pool temperature during reactor operation.

### 7.1.2 Identification of Safety Criteria

#### 7.1.2.1 General

Design bases and criteria for I&C equipment design are based on the need to have each system perform its intended function while meeting the requirements of applicable general design criteria, regulatory guides, industry standards, and other documents.

The safety design basis for a safety system states in functional terms the unique design requirements that establish the limits within which the safety objectives shall be met. The general functional requirement portion of the safety design basis presents those requirements which have been determined to be sufficient to ensure the adequacy and reliability of the system from a safety viewpoint. Many of these requirements have been incorporated into various codes, criteria, and regulatory requirements.

#### 7.1.2.1.1 Safety Design Bases for Safety Systems

Safety systems provide actions necessary to assure safe plant shutdown to protect the integrity of radioactive material barriers and / or prevent the release of radioactive material in excess of allowable dose limits. These safety systems consist of components, groups of components, systems, or groups of systems. A safety system may have a power generation design basis which states in functional terms the unique design requirements which establish the limits within which the power generation objective for the system shall be set.

#### 7.1.2.1.2 Specific Regulatory Requirements

The plant systems have been examined with respect to specific regulatory requirements and industry standards which are applicable to the instrumentation and controls for the various systems. Applicable requirements include specific parts or entities from the following:

(1) Title 10 Code of Federal Regulations

(2) Industry codes and standards

(3) NRC Regulatory Guides

The specific regulatory requirements identified in the Standard Review Plan which are applicable to each system instrumentation and control are specified in Table 7.1-2. For a discussion of the degree of conformance, see the analysis subsection for the specific system.

#### 7.1.2.1.3 Non-Safety Design Bases

Non-safety-related (including power-generation) systems are reactor support systems which are not required to protect the integrity of radioactive material barriers nor prevent the release of radioactive material in excess of allowable dose limits. The I&C portions of these systems may, by their actions, prevent the plant from exceeding preset limits which would otherwise initiate action of the safety systems.

#### 7.1.2.1.4 Instrument Errors

The design considers instrument drift, testability, and repeatability in the selection of instrumentation and controls and in the determination of setpoints. Adequate margin between safety limits and instrument setpoints is provided to allow for instrument error (safety limits, setpoints, and margins are provided in Chapter 16). The amount of instrument error is determined by test and experience. The setpoint is selected based on the known error. The recommended test frequency is greater on instrumentation that demonstrates a stronger tendency to drift.

##### 7.1.2.1.4.1 Safety System Setpoints

The safety system setpoints are listed in the Chapter 16 for each safety system. The settings are determined based on operating experience and conservative analyses. The settings are high enough to preclude inadvertent initiation of the safety action but low enough to assure that significant margin is maintained between the actual setting and the limiting safety system settings. Instrument drift, setting error, and repeatability are considered in the setpoint determination (Subsection 7.1.2.1.4). The margin between the limiting safety system settings and the actual safety limits includes consideration of the maximum credible transient in the process being measured.

The periodic test frequency for each variable is determined from historical data on setpoint drift and from quantitative reliability requirements for each system and its components.

#### 7.1.2.1.5 Technical Design Bases

The technical design bases for the RPS are provided in Section 7.2, engineered safety features in Section 7.3, systems required for safe shutdown in Section 7.4, and other systems required for safety in Section 7.6.

#### *7.1.2.1.6 [Protection System Inservice Testability*

*The RPS and ESF Systems can be tested during reactor operation by six separate tests. The first five tests are primarily manual tests and, although each individually is a partial test, combined with the sixth test they constitute a complete system test. The sixth test is the self-test of the safety system logic and control which automatically tests the complete system excluding sensors and actuators.*

*(1) The first of these is the manual scram test. The manual scram test verifies the ability to de-energize the scram pilot valve solenoids without scram by using the manual scram pushbutton switches. By depressing the manual scram button for one trip logic, half of the scram solenoids are de-energized. After the first trip logic is reset, the second trip logic is tripped manually to complete the test for the two manual scram buttons. In addition to control room and computer printout indications, scram group indicator lights indicate that the actuator trip logics have de-energized the scram pilot valve solenoids.*

*On the back panels, a separate, manual pushbutton switch in each of the four divisions provides a means to manually trip all trip actuators in that division. This sealed-in division manual trip is equivalent to a sealed-in automatic trip from the same division of trip logic. (An alternate manual scram can be accomplished by depressing any two or more of the four divisional manual trip pushbuttons.)*

*(2) The second test includes calibration of the Neutron Monitoring System (NMS) by means of simulated inputs from calibration signal units. Calibration and test controls for the NMS are located in the Control Building equipment room. They are under the administrative control of the control room operator and can be done either manually or automatically (see Subsection 7.6.1.1 for the calibration procedure).*

*(3) The third test is the single rod scram test which verifies the capability of each rod to scram. It is accomplished by operating switches for the particular control rod drive. Timing traces can be made for each rod scrammed. Prior to the test, a physics review is conducted to assure that the rod pattern during scram testing will not create a rod of unacceptable reactivity worth.*

*(4) The fourth test checks calibration of analog sensor inputs at the analog inputs of the remote multiplexing units. With a division-of-sensors bypass in place, calibrated, variable ramp signals are injected in place of the sensor signals and monitored at the SSLC control room panels for linearity, accuracy, fault response, and downscale and upscale trip response. The test signals are adjustable manually from the control room and also are capable of performing an automatic sequence of events. When surveillance testing during plant shutdown, trip coincidence and actuated device operation can be verified by simultaneous trip tests of coincident channels. Pressure transmitters and level transmitters are located on their respective local panels. The transmitters can be individually valved out of service and subjected to test pressure to verify operability of the transmitters as well as verification of calibration range. To gain access to the field controls on each transmitter, a cover plate or sealing device must be removed. Access to the field controls is granted only to qualified personnel for the purpose of testing or calibration adjustments.*

*(5) The fifth test is the sensor check. Digital inputs are tested by varying the monitored variable (e.g., stop valve closure, control valve fast closure, main steamline isolation valve closure) or by substituting a test source for the sensor from the process variable and varying the source. In those cases where the sensor is disconnected from the process variable, an out-of-service alarm will be indicated in the main control room. Analog input is checked by cross comparison of the instrument channels measuring the same variable.*

*(6) The sixth test is an integrated self-test provision built into the microprocessors within the SSLC. It consists of an online, continuously operating, self-diagnostic monitoring network, and an offline semi-automatic (operator initiated, but automatic to*

*completion), end-to-end surveillance program. Both online and offline functions operate independently within each of the four divisions. There are no multi-divisional interconnections associated with self-testing.*

*The primary purpose of the self-test is to improve the availability of the SSLC by optimizing the time to detect and determine the location of a failure in the functional system. It is not intended that the self-test eliminate the need for the other five manual tests. However, most faults are detected more quickly than with manual testing alone.*

*The self-test function is classified as safety-related. Its hardware and software are an integral part of the SSLC and, as such, are qualified to Class 1E standards.*

*The hierarchy of test capability is provided to ensure maximum coverage of all EMS/SSLC functions, including logic functions and data communications links. Testing shall include:*

*(a) Online Continuous Testing*

*A self-diagnostic program monitors each signal processing module from input to output. Testing is automatic and is performed periodically during normal operation. Tests will verify the basic integrity of each card or module on the microprocessor bus. All operations are part of normal data processing intervals and will not affect system response to incoming trip or initiation signals. Automatic initiation signals from plant sensors will override an automatic test sequence and perform the required safety function. Process or logic signals are not changed as a result of self-test functions.*

*Self-diagnosis includes monitoring of overall program flow, reasonableness of process variables, RAM and PROM condition, and device interlock logic. Testing includes continuous error checking of all transmitted and received data on the serial data links of each SSLC controller; for example, error checking by parity check, checksum, or cyclic redundancy checking (CRC) techniques.*

*A fault is considered the discrepancy between an expected output of a permissive circuit and the existing present state.*

*Actuation of the trip function is not performed during this test. The self-test function is capable of detecting and logging intermittent failures without stopping system operation. Normal surveillance by plant personnel will identify these failures, via a diagnostic display, for preventive maintenance.*

*Self-test failures (except intermittent failures) are annunciated to the operator at the main control room console and logged by the process computer. Faults are identified to the replacement board or module level and positively indicated at the failed unit.*

*The continuous surveillance monitoring also includes power supply voltage levels, card-out-of-file interlocks, and battery voltage levels on battery-backed memory cards (if used). Out-of-tolerance conditions will result in an inoperative (out-of-service) condition for that particular system function.*

*Automatic system self-testing occurs during a portion of every periodic transmission period of the data communication network. Since exhaustive tests cannot be performed during any one transmission interval, the test software is written so that sufficient overlap coverage is provided to prove system performance during tests of portions of the circuitry, as allowed in IEEE 338.*

*The Essential Multiplexing System (EMS) is included in the continuous, automatic self-test function. Faults at the Remote Multiplexing Units (RMUs) are alarmed in the main control room. Since the EMS is dual in each division, self-test supports automatic reconfiguration or bypass of portions of EMS after a detected fault, such that the least effect on system availability occurs.*

*(b) Offline Semi-automatic End-to-End (Sensor Input to Trip Actuator) Testing*

*The more complete, manually-initiated, internal self-test is available when a unit is offline for surveillance or maintenance testing. This test exercises the trip outputs of the SSLC logic processors. The channel containing the processors will be bypassed during testing.*

*A fault is considered the inability to open or close any control circuit.*

*Self-test failures are displayed on a front panel readout device or other diagnostic unit.*

*To reduce operator burden and decrease outage time, a surveillance test controller (STC) is provided as a dedicated instrument in each division of SSLC. The STC performs semi-automatic (operator-initiated) testing of SSLC functional logic, including trip, initiation, and interlock logic. Test coverage includes verification of correct operation of the following capabilities, as defined in each system IBD:*

*(i) Each 2/4 coincident logic function.*

*(ii) Serial and parallel I/O, including manual control switches, limit switches, and other contact closures.*

*(iii) The 1/N trip selection function.*

*(iv) Interlock logic for each valve or pump.*

*A separate test sequence for each safety system is operator-selectable; testing will proceed automatically to conclusion after initiation by the operator. Surveillance testing is performed in one division at a time. The surveillance test frequency is given in Chapter 16.*

*The STC injects test patterns through the EMS communications links to the RMUs. It then tests the RMUs' ability to format and transmit sensor data through and across the EMS/SSLC interface, in the prescribed time, to the load drivers. Under the proper bypass conditions, or with the reactor shut down, the load drivers themselves may be actuated.*

*All testing features adhere to the single-failure criterion, as follows: (1) No single failure in the test circuitry shall incapacitate an SSLC safety function. (2) No single failure in the test circuitry shall cause an inadvertent scram, MSIV isolation, or actuation of any safety systems served by the SSLC.* ]*

### 7.1.2.2 Reactor Protection (Trip) System (RPS)—Instrumentation and Controls

(1) Safety Design Bases (Conformance to the following design bases is discussed in Section 7.2.2.1).

The Reactor Protection (trip) System (RPS) shall meet the following functional requirements:

(a) Initiate a reactor scram with precision and reliability to prevent or limit fuel damage following abnormal operational transients.

(b) Initiate a scram with precision and reliability to prevent damage to the reactor coolant pressure boundary as a result of excessive internal pressure (i.e., to prevent nuclear system pressure from exceeding the limit allowed by applicable industry codes).

(c) Limit the uncontrolled release of radioactive materials from the fuel assembly or reactor coolant pressure boundary, by precisely and reliably initiating a reactor scram on gross failure of either of these barriers.

(d) Detect conditions that threaten the fuel assembly or reactor coolant pressure boundary from inputs derived from variables that are true, direct measures of operational conditions.

(e) Respond correctly to the sensed variables over the expected range of magnitudes and rates of change.

(f) Provide a sufficient number of sensors for monitoring essential variables that have spatial dependence.

The following design bases assure RPS reliability:

(g) If a single random failure can cause a control system action that causes a plant condition that requires a reactor scram but also prevents action

* See Subsection 7.1.1.2.

by some RPS channels, the remaining portions of the RPS shall meet the functional requirements (items a, b and c above), even when degraded by a second random failure.

(h) Loss of one power supply shall neither directly cause nor prevent a reactor scram.

(i) Once initiated, an RPS action shall go to completion. Return to normal operation shall require deliberate operator action.

(j) There shall be sufficient electrical and physical separation between redundant I&C equipment monitoring the same variable to prevent environmental factors, electrical transients, or physical events from impairing the ability of the system to respond correctly.

(k) Not used

(l) No single failure within the RPS shall prevent proper RPS action when required to satisfy Safety Design Bases as described by a, b, and c above.

(m) Any one intentional bypass, maintenance operation, calibration operation, or test to verify operational availability shall not prevent the ability of the reactor protection system to respond correctly.

(n) The system shall be designed so that two or more sensors for any monitored variable exceeding the scram setpoint will initiate an automatic scram.

The following bases reduce the probability that RPS operational reliability and precision will be degraded by operator error:

(o) Access to trip settings, component calibration controls, test points, and other terminal points shall be under the control of plant operations supervisory personnel.

(p) Manual bypass of instrumentation and control equipment components shall be under the control of the control room operator. If the ability to trip some essential part of the system has been bypassed, this fact shall be continuously annunciated in the main control room.

(q) Provides selective automatic and manual operational trip bypasses, as necessary, to permit proper plant operation. Those bypasses allow for protection requirements that depend upon specific existing or subsequent reactor operating conditions.

(r) Provides manual control switches for initiation of reactor scram by plant operator when necessary.

(s) Provides mode selection for enabling the appropriate instrument channel trip functions required in a particular mode of operation.

Specific regulatory requirements:

Specific requirements applicable to the RPS instrumentation and control are shown in Table 7.1-2.

(2) Non-Safety-Related Design Bases

The RPS is designed with the added objective of plant availability. The setpoints, power sources, and instrumentation and controls shall be arranged in such a manner as to preclude spurious scrams insofar as practicable and safe.

### 7.1.2.3 Engineered Safety Features (ESF)

#### 7.1.2.3.1 Emergency Core Cooling Systems—Instrumentation and Controls

(1) Safety Design Bases

General Functional Requirements:

The ECCS instrumentation and controls shall be designed to meet the following requirements:

(a) Automatically initiate and control the ECCS to prevent fuel cladding temperatures from reaching the limits of 10CFR50.46.

(b) Respond to a need for emergency core cooling regardless of the physical location of the malfunction or break that causes the need.

(c) Limit dependence on operator judgment in times of stress by:

(i) Automatic response of the ECCS so that no action is required of plant operators within 30 minutes after a loss-of-coolant accident.

(ii) Indication of performance of the ECCS by main control room instrumentation.

(iii) Provision for manual control of the ECCS in the main control room.

Specific Regulatory Requirements:

Specific regulatory requirements applicable to the instrumentation and controls for the ECCS are shown on Table 7.1-2.

(2) Non-safety-Related Design Bases

None.

### 7.1.2.3.2 Leak Detection and Isolation System (LDS)—Instrumentation and Controls

(1) Safety Design Bases

The general functional requirements of the LDS instrumentation and controls are to detect, indicate and alarm leakage from the reactor primary pressure boundary and, in certain cases, to initiate closure of isolation valves to shut off leakage external to the containment.

In order to meet the safety design basis, the LDS I&C system shall be designed (as a minimum) to:

(a) Provide direct and accurate measurements of parameters which are indicative of a reactor coolant pressure boundary (RCPB) leak or a leak of reactor coolant outside the containment and then provide automatic isolation of the affected system or area.

(b) Monitor predetermined parameters with precision and reliability and respond correctly to the sensed parameters.

(c) Provide a sufficient number of independent monitors, sensing each parameter to ensure accurate measurement and preclude the possibility of a failure to isolate due to instrumentation failure.

(d) Provide an isolation control system with sufficient redundancy to ensure that the LDS can perform its intended function, assuming a single failure caused by any of the design basis events or a single power supply failure.

(e) Provide an isolation control system which will ensure that isolation of the containment and/or reactor vessel will occur once initiated.

(f) Provide instrumentation and control to permit the operator to manually initiate isolation if necessary.

(g) Provide interlocks to assure reset capability is only possible after clearance of isolation signals.

Specific Regulatory Requirements:

Specific regulatory requirements applicable to this system are shown in Table 7.1-2.

(2) Non-Safety-Related Design Bases

The LDS instrumentation and controls are designed to:

(a) Provide sufficient redundancy of instruments to avoid unnecessary plant shutdowns due to instrument malfunctions.

(b) Avoid plant shutdowns due to a single power supply failure.

(c) Provide the capability to maintain, calibrate, or adjust system monitors while operating without causing plant shutdowns or reducing safety margins.

(d) Provide status information to the process computer and for annunciation of excessive leakage.

### 7.1.2.3.3 RHR Wetwell and Drywell Spray Cooling Mode—Instrumentation and Controls

(1) Safety Design Bases

The general functional requirements of the wetwell and drywell cooling mode of the RHR System shall provide instrumentation and controls to:

(a) Initiate wetwell and drywell spray as required to avoid environmental conditions of pressure and temperature that would threaten the integrity of the containment during a transient or accident condition.

(b) Sense wetwell and drywell pressure and permit manual system initiation in order to provide condensation of steam in the wetwell and drywell air volumes during a transient or accident event.

(c) Manually control the wetwell and drywell spray subsystem in the main control room.

(d) Indicate performance of the wetwell and drywell spray subsystem in the main control room.

Specific Regulatory Requirements:

Specific regulatory requirements applicable to the containment spray system are listed in Table 7.1-2.

(2) Non-safety-Related Bases

None.

### 7.1.2.3.4 RHR Suppression Pool Cooling Mode—Instrumentation and Controls

(1) Safety Design Bases

General Functional Requirements:

The general functional requirements of the instrumentation and controls cause automatic initiation of suppression pool cooling upon sensed high temperature in the suppression pool. The reactor operator may also manually initiate suppression pool cooling to ensure that the pool temperature does not exceed the preestablished pool temperature immediately after any steam discharge to the pool.

Specific Regulatory Requirements:

Specific regulatory requirements are listed in Table 7.1-2.

(2) Non-Safety-Related Design Bases

None.

### 7.1.2.3.5 Standby Gas Treatment System—Instrumentation and Controls

(1) Safety Design Bases

General Functional Requirements:

The general functional requirements of the instrumentation and controls of this system shall maintain a negative pressure in the secondary containment, relative to the outdoor atmosphere, in order to control exfiltration of fission products after either (a) a loss-of-coolant accident (LOCA) or (b) a high level of radioactivity in the secondary containment exhaust. The system also filters airborne radioactivity (particulate and halogen) in the effluent to reduce post-accident offsite exposure.

Specific Regulatory Requirements:

The specific regulatory requirements applicable to this system are given in Table 7.1-2.

(2) Non-safety-Related Design Bases

(a) Process gaseous effluent from the primary containment and secondary containment when required to limit the discharge of radioactivity to the environment during normal and abnormal plant operations.

(b) Maintain the secondary containment at a negative pressure following a loss of offsite power.

### 7.1.2.3.6 Emergency Diesel Generator Support Systems—Instrumentation and Controls

(1) Safety Design Bases

General Functional Requirements:

The general functional requirements of the instrumentation and controls for the diesel generator and its auxiliaries and support systems assure the automatic startup and continued operation of the diesel generator units of the plant standby power system under emergency or DBA conditions.

Specific Regulatory Requirements:

Specific regulatory requirements applicable to the diesel generator and its auxiliaries are listed in Table 7.1-2.

(2) Non-Safety-Related Design Bases

There is no power generation design basis for this system.

### 7.1.2.3.7 Reactor Building Cooling Water System—Instrumentation and Controls

(1) Safety Design Bases

General Functional Requirements:

The general functional requirements of the instrumentation and controls of this system shall be to:

(a) Maintain control of cooling water to equipment that requires cooling during reactor shutdown modes and following a LOCA or LOPP or both.

(b) Provide for the automatic isolation of the non-essential parts of the Reactor Building Cooling Water (RCW) System (except CRD pump oil coolers and instrument air coolers) from the essential parts during a LOCA or upon detection of a major RCW leak in the non-essential system.

Specific Regulatory Requirements:

Specific regulatory requirements applicable to the system instrumentation and controls are given in Table 7.1-2.

(2) Non-Safety-Related Design Bases

(a) Instrumentation and controls shall be provided to monitor and control the distribution of reactor building cooling water to remove heat from plant auxiliaries during normal plant operation.

(b) The RCW shall be capable of being tested during normal plant operation.

#### 7.1.2.3.8 Essential HVAC Systems—Instrumentation and Controls

(1) Safety Design Bases

See Subsections 9.4.1.1.1 and 9.4.5.1.1.

#### 7.1.2.3.9 HVAC Emergency Cooling Water System—Instrumentation and Controls

(1) Safety Design Bases

General Functional Requirements:

The general functional requirements of the HVAC Emergency Cooling Water System instrumentation and controls shall provide control for cooling units that ensure a controlled environment for essential equipment and control room areas following a loss-of-coolant accident, loss of preferred power, or isolation of normal heating, venting, and air conditioning (HVAC). See Subsection 7.8.1 for COL license information.

Specific Regulatory Requirements:

Specific regulatory requirements applicable to the system instrumentation and control are given in Table 7.1-2.

(2) Non-Safety-Related Design Bases

The system shall provide a continuous supply of chilled water to the cooling coils of air conditioning systems which provide a controlled temperature environment and proper humidity to ensure the comfort of the operating personnel and to provide a suitable atmosphere for the operation of control equipment.

#### 7.1.2.3.10 High Pressure Nitrogen Gas Supply System—Instrumentation and Control

(1) Safety Design Bases

General Functional Requirements:

The general functional requirements of the instrumentation and controls shall provide automatic and manual control of the nitrogen gas supply to assure its operation during all modes of plant operation, and to automatically initiate the emergency nitrogen bottle supply (on low nitrogen supply pressure) to assure adequate supply of nitrogen to automatic depressurization

safety / relief valves and to nitrogen-using equipment and valves in the reactor building.

Specific Regulatory Requirements:

Specific regulatory requirements applicable to this system are listed in Table 7.1-2.

(2) Non-Safety-Related Design Bases

There is no power generation design basis for this system.

### 7.1.2.4 Safe Shutdown Systems—Instrumentation and Controls

#### 7.1.2.4.1 Alternate Rod Insertion Function (ARI)—Instrumentation and Controls

(1) Safety Design Bases

None.

(2) Non-safety-Related Design Bases

The general functional requirements of the instrumentation and controls of the ARI function are to:

(a) Provide alternate and diverse method for inserting control rods using fine motion control rod drive (FMCRD) electric motors.

(b) Provide for automatic and manual operation of the system.

(c) Provide assurance that the ARI shall be highly reliable and functional in spite of a single failure.

(d) Provide assurance that the ARI shall operate when necessary (FMCRD motors shall be connected to the emergency diesel generators).

(e) Mitigate the consequences of anticipated transient without scram (ATWS) events.

#### 7.1.2.4.2 Standby Liquid Control System (SLCS)—Instrumentation and Controls

(1) Safety Design Bases

General Functional Requirements:

The general functional requirements of this equipment are to provide necessary control of the SLC equipment for shutting the reactor down from full power to cold shutdown and maintaining the reactor in a subcritical state

at atmospheric temperature and pressure conditions by pumping sodium pentaborate (a neutron absorber) into the reactor.

Specific Regulatory Requirements:

Specific regulatory requirements applicable to this system are given in Table 7.1-2.

(2) Non-Safety-Related Design Bases

None.

#### 7.1.2.4.3 RHR—Reactor Shutdown Cooling Mode—Instrumentation and Controls

(1) Safety Design Bases

General Functional Requirements:

The general functional requirements of the shutdown cooling mode of the RHR are to provide monitoring and control as required to:

(a) Enable the system to remove the residual heat (decay heat and sensible heat) from the reactor vessel during normal shutdown.

(b) Provide manual controls for the shutdown cooling system in the main control room and at the remote shutdown panel.

(c) Indicate performance of the shutdown cooling system by main control room instrumentation and controls in the remote shutdown panel.

Specific Regulatory Requirements:

Specific regulatory requirements applicable to reactor shutdown cooling are given in Table 7.1-2.

(2) Non-Safety-Related Design Bases

The I&C System shall provide monitoring the control to enable the RHR System to accomplish the following:

(a) Provide cooling for the reactor during the shutdown operation when the vessel pressure is below approximately 931.63 kPa G.

(b) Cool the reactor water to a temperature which is practical for refueling and servicing operation.

#### 7.1.2.4.4 Remote Shutdown System (RSS)—Instrumentation and Controls

(1) Safety Design Bases

General Functional Requirements:

The general functional requirements of the Remote Shutdown System (RSS) I&C shall provide the following:

(a) 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.

(b) Capability for subsequent cold shutdown of the reactor through the use of suitable procedures.

Specific Regulatory Requirements:

Specific regulatory requirements applicable to the remote shutdown system are listed in Table 7.1-2.

(2) Non-Safety-Related Design Bases

None.

### 7.1.2.5 Safety-Related Display Instrumentation

(1) Safety Design Bases

General Functional Requirements:

The general functional requirements are the necessary display instrumentation in the main control room so the reactor operator can determine and accomplish the manual control actions required for safe plant operation.

Specific Regulatory Requirements:

The specific regulatory requirements applicable to the safety-related display instrumentation are listed in Table 7.1-2.

(2) Non-Safety-Related Design Bases

Sufficient and reliable display instrumentation shall be provided so that all the expected power operation actions and maneuvers can be reasonably accomplished by the reactor operator from the main control room.

### 7.1.2.6 Other Safety-Related Systems

### 7.1.2.6.1 Neutron Monitoring System (NMS)—Instrumentation and Controls

#### 7.1.2.6.1.1 Startup Range Neutron Monitoring (SRNM) Subsystem

(1) Safety Design Bases

General Functional Requirements:

(a) The SRNM Subsystem shall generate a high neutron flux trip signal or a short period trip signal that can be used to initiate scram in time to prevent fuel damage resulting from anticipated or abnormal operational transients.

(b) The SRNM Subsystem and its preamplifier shall be qualified to operate under accident and abnormal environmental conditions.

(c) The independence and redundancy incorporated in the SRNM functional design shall be consistent with the safety design basis of the Reactor Protection System (Section 7.1.2.2).

Specific Regulatory Requirements:

Specific regulatory requirements for the NMS SRNM Subsystem are on Table 7.1-2.

(2) Non-safety-Related Design Bases

The SRNM Subsystem meets the following non-safety-related design bases:

(a) Neutron sources and neutron detectors together shall result in a signal-to-noise ratio of at least 2:1 and a signal count rate of at least three counts per second with all control rods fully inserted in a cold unexposed core.

The SRNM Subsystem shall be able to perform the following functions:

(a) Indicate a measurable increase in output signal from at least one detecting channel before the reactor period is less than 20 seconds during the worst possible startup rod withdrawal conditions.

(b) Indicate measurable increases in output signals with the maximum permitted number of SRNM channels out of service during normal reactor startup operations.

(c) Provide a continuous monitoring of the neutron flux over a range of ten decades (approximately $1 \times 10^3$ neutron/$cm^2$ to $1.5 \times 10^{13}$ neutron/$cm^2$).

(d) Provide a continuous measure of the time rate of change of neutron flux (reactor period) over the range from –100 s to (–) infinity and (+) infinity to +10 s.

(e) Generate interlock signals to block control rod withdrawal if the neutron flux is greater than or less than preset values or if certain electronic failures occur.

(f) Generate rod block whenever the period exceeds the preset value.

(g) Except for annunciators, the loss of a single power bus shall not disable the monitoring and alarming functions of all the available monitors.

#### 7.1.2.6.1.2 Flow Rate Subsystem

(1) Safety Design Bases

General Functional Requirements:

The flow rate subsystem, as part of the APRM Subsystem, provides the control and reference signal for the APRM core flow-rate dependent trips. It consists of a flow measurement from the recirculation system and signal conditioning equipment.

Specific Regulatory Requirements:

Specific regulatory requirements applicable to the controls and instrumentation for the Neutron Monitoring System are listed in Table 7.1-2.

(2) Non-Safety-Related Design Bases

None.

### 7.1.2.6.1.3 Local Power Range Monitor (LPRM) Subsystem

(1) Safety Design Bases

General Functional Requirements:

General functional requirements of the LPRM Subsystem are a sufficient number of LPRM signals to satisfy the APRM safety design bases.

Specific Regulatory Requirements:

Specific regulatory requirements applicable to the controls and instrumentation for the Neutron Monitoring System are shown in Table 7.1-2.

(2) Non-Safety-Related Design Bases

The LPRM supplies the following:

(a) Signals to the APRM that are proportional to the local neutron flux at various locations within the rector core.

(b) Signals to alarm high or low local neutron flux.

(c) Signals proportional to the local neutron flux to drive indicating meters and auxiliary devices to be used for operator evaluation of power distribution, local heat flux, minimum critical power, and fuel burnup rate.

### 7.1.2.6.1.4 Average Power Range Monitor (APRM) Subsystem

(1) Safety Design Bases

General Functional Requirements:

The general functional requirements are that, under the worst permitted input LPRM bypass conditions, the APRM Subsystem shall be capable of generating a trip signal in response to average neutron flux increases in time to prevent fuel damage. The APRM generator trip functions with trip inputs to the RPS also include: simulated thermal power trip, APRM inoperative trip, core flow rapid decrease trip, and core power oscillation trip of the oscillation power range monitor (OPRM). The OPRM design basis is to provide a trip to prevent growing core flux oscillation to prevent thermal limit violation, while discriminating against false signals from other signal fluctuations not related to core instability. The independence and redundancy incorporated into the design of the APRM Subsystem shall be consistent with the safety design bases of the Reactor Protection System(RPS). The RPS design bases are discussed in Subsection 7.1.2.2.

Specific Regulatory Requirements:

Specific regulatory requirements applicable to the controls and instrumentation for the neutron monitoring system are listed in Table 7.1-2.

(2) Non-Safety-Related Design Bases

The APRM shall provide the following functions:

(a) A continuous indication of average reactor power (neutron flux) from a 1% to 125% of rated reactor power which shall overlap with the SRNM range.

(b) Interlock signals for blocking further rod withdrawal to avoid an unnecessary scram actuation.

(c) A reference power level to the Reactor Recirculation System.

(d) A simulated thermal power signal derived from each APRM channel which approximates the dynamic effects of the fuel.

(e) A continuous LPRM/APRM display for detection of any neutron flux oscillation in the reactor core. This includes the flux oscillation detection algorithm incorporated in the APRM Subsystem.

(f) A reference power level to permit trip in response to a reactor internal pump trip.

#### 7.1.2.6.1.5 Automated Traversing Incore Probe (ATIP) Subsystem

(1) Safety Design Bases

None. The ATIP Subsystem portion of the NMS is non-safety-related and is addressed in Section 7.7

(2) Non-Safety-Related Design Bases

The ATIP shall meet the following power generation design bases:

(a) Provide a signal proportional to the axial neutron flux distribution at the radial core locations of the LPRM detectors (this signal shall be of high precision to allow reliable calibration of LPRM gains).

(b) Provide accurate indication of the axial position of the flux measurement to allow pointwise or continuous measurement of the axial neutron flux distribution.

(c) Provide a totally automated mode of operation by the computer-based automatic control system.

#### 7.1.2.6.1.6 Multi-Channel Rod Block Monitor (MRBM) Subsystem

(1) Safety Design Basis

None, the MRBM Subsystem portion of the NMS is non-safety-related and is addressed in Section 7.7.

(2) Non-Safety-Related Design Basis

The MRBM Subsystem shall meet the following power generation design bases:

(a) Provide a signal proportional to the average neutron flux level surrounding the control rod(s) being withdrawn.

(b) Issue a rod block signal if the preset setpoint is exceeded by this signal which is proportional to the average neutron flux level signal.

### 7.1.2.6.2 Process Radiation Monitoring System

(1) Safety Design Bases

General Functional Requirements:

(a) Monitor the gross radiation level in the main steamlines tunnel area and in the ventilation discharge ducting of the primary and secondary containment structures.

(b) Provide radiation measurement, display, recording and alarm capability in the main control room.

(c) Provide alarm annunciation signals to the main control room if alarm or trip levels are reached or the subsystem is in an inoperative condition.

(d) Provide channel trip inputs to the RPS and LDS on high radiation in the MSL tunnel area. If the protection system logic is satisfied, the following shall be initiated:

(i) Reactor scram.

(ii) Closure of the main steamline isolation valves.

(iii) Shutdown of the mechanical vacuum pump and closure of the mechanical pump discharge line isolation valve.

(e) Provide trip signals to isolate the secondary containment, and to initiate the SGTS on high radiation levels in the exhaust ducts of the fuel handling area or in the Reactor Building.

(f) Monitor the intake air supply to the Control Building so habitability of the control room can be maintained during an accident condition.

(g) Provide channel trip inputs to the safety system and logic control (SSLC) system for logic voting and subsequent initiation of protective actions.

(2) Non-safety-Related Design Bases

(a) Monitor the gross level of radioactive material in liquid effluent streams which may contain radioactive materials, and in selected liquid process streams associated with liquid effluent streams.

(b) Monitor the gaseous effluent streams which may contain radioactive material and at selected locations in the offgas system.

(c) Provide sampling capability for radioactive iodines and particulates in gaseous and effluent streams which may contain radioactive material.

(d) Provide radiation measurement, display, recording and alarm capability in the main control room.

(e) Provide alarm annunciation signals to the main control room if alarm or trip levels are reached or the radiation monitoring subsystem becomes inoperative, and provide input to the offgas system when the radioactive gas concentration in the offgas system discharge is at or in excess of the restrictive concentration limit derived from Technical Specification release rate limits and that discharge from the offgas system must be terminated.

(f) Provide input to the radwaste system indicating that radioactive material concentration in the radwaste system discharge is at or in excess of a predetermined setpoint and that discharge from the radwaste system must be terminated.

### 7.1.2.6.3 High Pressure/Low Pressure Interlock Function

(1) Safety Design Bases

The general functional requirements are to protect the low pressure system boundary from postulated overpressurization from the reactor system.

(2) Non-Safety-Related Design Bases

None.

### 7.1.2.6.4 Not Used

### 7.1.2.6.5 Wetwell-to-Drywell Vacuum Breaker System—Instrumentation and Controls

See Subsection 6.2.1.1.4.

### 7.1.2.6.6 Containment Atmospheric Monitoring (CAM) Systems

(1) Safety Design Bases

General Functional Requirements:

Monitor the atmosphere in the inerted primary containment for radiation levels and for concentration of hydrogen and oxygen gases, primarily during post-accident conditions. Monitoring shall be provided by two independent safety-related divisional subsystems.

Monitor continuously the radiation environment in the drywell and suppression chamber during reactor operation and under post-accident conditions.

Sample and monitor the oxygen and hydrogen concentration levels in the drywell and suppression chamber under post-accident conditions, and also when required during reactor operation. The LOCA signal (low reactor water level or high drywell pressure) shall activate the system and place it into service to monitor the gaseous buildup in the primary containment following an accident.

Specific Regulatory Requirements:

Specific regulatory requirements applicable to this system are listed in Table 7.1-2.

(2) Non-Safety-Related Design Bases

Separate hydrogen and oxygen gas calibration sources shall be provided for each CAM Subsystem for periodic calibration of the gas analyzers and monitors.

### 7.1.2.6.7 Suppression Pool Temperature Monitoring System—Instrumentation and Control

(1) Safety Design Bases

General Functional Requirements:

The SPTM is a Class 1E safety-related system. The general functional requirements shall be to automatically initiate suppression pool cooling or scram the reactor when high suppression pool temperatures are detected that might be caused by safety relief valve leakage or malfunction.

Specific Regulatory Requirements:

The specific regulatory requirements applicable to this system are listed in Table 7.1-2.

(2) Non-Safety-Related Design Bases

None.

### 7.1.2.7 Control Systems Not Required For Safety

(1) Safety Design Bases

These systems have no functional safety design bases; however, they are designed so that the functional capabilities of safety-related systems are not precluded.

(2) Regulatory Requirements

Specific regulatory requirements applicable to those systems are listed in Table 7.1-2.

### 7.1.2.8 Independence of Safety-Related Systems

(See Subsections 8.3.1.3 and 8.3.1.4.)

### 7.1.2.9 Conformance to Regulatory Requirements

#### 7.1.2.9.1 Regulation 10CFR50.55a

The only portion of 10CFR50.55a applicable to the I&C equipment is 10CFR50.55a(h), which requires the application of IEEE 279 for protection systems (Subsection 7.1.2.11.1).

#### 7.1.2.9.2 Regulation 10CFR50 Appendix A

Conformance with NRC General Design Criteria is discussed for all structures, components, equipment and systems in Section 3.1. Further clarification and discussion of the I&C systems themselves are provided in Sections 7.2 through 7.7. Individual systems application to GDCs identified in the Standard Review Plan for Chapter 7 are shown on Table 7.1-2.

### 7.1.2.10 Conformance to Regulatory Guides

The following compliance statements for Regulatory Guides applicable to I&C describe the generic basis for their application. Individual system application is identified on Table 7.1-2 and discussed in the analysis portions of Sections 7.2 through 7.7.

#### 7.1.2.10.1 Regulatory Guide 1.22—Periodic Testing of Protection System Actuation Functions

All safety-related systems have provision for periodic testing. Proper functioning of analog sensors can be verified by channel cross-comparison. Some actuators and digital sensors, because of their locations, cannot be fully tested during actual reactor operation. Such equipment is identified and provisions for meeting the requirements of Paragraph D.4 (per BTP ICSB 22) are discussed in the analysis portions of Sections 7.2, 7.3, 7.4 and 7.6.

#### 7.1.2.10.2 Regulatory Guide 1.47—Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems

Bypass indications are designed to satisfy the requirement of IEEE 279, Paragraph 4.13, Regulatory Guide 1.47, and BTP ICSB 21. Additional information may be found in the system detail descriptions in Sections 7.2, 7.3, 7.4 and 7.6. The design of the bypass indications allows testing during normal operation and is used to supplement administrative procedures by providing indications of safety systems status.

Bypass indications are designed and installed in a manner which precludes the possibility of adverse affects on the plant safety system. Those portions of the bypass indications which, when faulted, could reduce the independence between redundant safety systems are electrically isolated from the protection circuits.

#### 7.1.2.10.3 Regulatory Guide 1.53—Application of the Single-Failure Criterion to Nuclear Power Plant Protection systems

The safety-related system designs conform to the single-failure criterion. The applicable system descriptions or analysis portions of Sections 7.2, 7.3, 7.4, and 7.6 provide further discussion.

#### 7.1.2.10.4 Regulatory Guide 1.62—Manual Initiation of Protective Actions

Manual initiation of the protective action is provided at the system level for all safety systems, including RPS, all ESF, and all other systems required for safety.

#### 7.1.2.10.5 Regulatory Guide 1.75—Physical Independence of Electric Systems

The safety-related systems described in Sections 7.2, 7.3, 7.4, and 7.6 comply with the independence and separation criteria for redundant systems in accordance with Regulatory Guide 1.75 or by implementation of the following alternates:

(1) Associated circuits installed in accordance with IEEE 384, Section 5.5.2(1), are subject to the requirements of Class 1E circuits for cable derating, environmental qualification, flame retardance, splicing restrictions, and raceway fill unless it is demonstrated that Class 1E circuits are not degraded below an acceptable level by the absence of such requirements.

(2) The method of identification used (IEEE 384, Section 6.1.2) will preclude the need to frequently consult any reference material to distinguish between Class 1E and non-Class 1E circuits, between non-Class 1E circuits associated with different redundant Class 1E systems, and between redundant Class 1E systems.

(3) First sentence of IEEE 384, Section 6.8 is implemented as follows:

Redundant Class 1E sensors and their connections to the process system shall be sufficiently separated that required functional capability of the protection system will be maintained despite any single design basis event.

(4) Non-Class 1E instrumentation circuits can be exempted from the provisions of IEEE 384, Section 5.6, provided they are not routed in the same raceway as power and control cables or are not routed with associated cables of a redundant division.

#### 7.1.2.10.6 Regulatory Guide 1.89—Environmental Qualification of Class 1E Equipment for Nuclear Power Plants

Qualification of Class 1E equipment is discussed in Chapter 3. Qualification tests and analyses are discussed in Subsection 3.11.2.

#### 7.1.2.10.7 Regulatory Guide 1.97—Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant Conditions During and Following an Accident

Instrumentation and controls are designed to meet the requirements of Regulatory Guide 1.97. Details of design implementation are discussed in Section 7.5.

#### 7.1.2.10.8 Regulatory Guide 1.100—Seismic Qualification of Electric Equipment for Nuclear Power Plants

All Class 1E equipment will meet the requirements of IEEE 344 and will be seismically qualified in conformance with Regulatory Guide 1.100, as discussed in Section 3.10.

#### 7.1.2.10.9 Regulatory Guide 1.105—Instrument Setpoints

[*Table 9 of DCD/Introduction identifies the commitments to use Regulatory Guide 1.105, which, if changed, requires NRC Staff review and approval prior to implementation. The applicable portions of the Tier 2 sections and tables, identified on Table 9 of DCD/Introduction for this restriction, are italicized on the sections and tables themselves.*]*

The I&C systems are consistent with the requirements of Regulatory Guide 1.105. The trip setpoint (instrument setpoint) allowance value (Tech Spec limit) and the analytical or design basis limit are all contained in the Technical Specifications (Chapter 16). These parameters are all appropriately separated from each other based on instrument accuracy, calibration capability and design drift (estimated) allowance data. The

* See Section 3.5 of DCD/Introduction.

setpoints are within the instrument best accuracy range. The established setpoints provide margin to satisfy both safety requirements and plant availability objectives.

#### 7.1.2.10.10 Regulatory Guide 1.118—Periodic Testing of Electric Power and Protection Systems

The I&C systems are consistent with the requirements of Regulatory Guide 1.118, with the following clarifications of the regulatory guide requirements:

(1) Position C.6b—Trip of an associated protective channel or actuation of an associated Class 1E load group is required on removal of fuses or opening of a breaker only for the purpose of deactivating instrumentation or control circuits.

(2) Position C.2—Insofar as is practical and safe, response time testing will be performed from sensor inputs (at the sensor input connection for process instruments) to and including the actuated equipment. Testability features are discussed in Subsection 7.1.2.1.6.

#### 7.1.2.10.11 Regulatory Guide 1.151—Instrument Sensing Lines

The instrument sensing lines are designed to meet the requirements of Regulatory Guide 1.151. Such lines are used to perform both safety and non-safety functions. However, there are four redundant and separate sets of instrument lines, each having Class 1E instruments associated with one of the four electrical Class 1E divisions. The RPS logic requires any two out of the four signals to scram. If a channel is bypassed, the logic is two-out-of-three. Also, emergency core cooling functions are redundant throughout the four divisions and the feedwater system is designed with fault-tolerant triplicated digital controllers. Therefore, the systems are designed such that no single failure could cause an event and at the same time prevent mitigating action for the event.

### 7.1.2.11 Conformance to Industry Standards

#### 7.1.2.11.1 IEEE 279—Criteria for Protection Systems for Nuclear Power Generating Stations

All safety-related systems are designed to meet the requirements of IEEE 279. Clarifications of any of the provisions are discussed for the applicable systems in the analysis portions of Sections 7.2, 7.3, 7.4, and 7.6.

#### 7.1.2.11.2 IEEE 323—Qualifying Class 1E Equipment for Nuclear Power Generating Stations

Written procedures and responsibilities are developed for the design and qualification of all Class 1E electrical equipment. This includes preparation of specifications, qualification procedures, and documentation as required. Whenever possible,

qualification testing or analysis is accomplished prior to release of the engineering design for production. Standards manuals are maintained containing specifications, practices, and procedures for implementing qualification requirements, and an auditable file of qualification documents is available for review (Section 3.11).

#### 7.1.2.11.3 IEEE 338—Standard Criteria for Periodic Testing or Nuclear Power Generating Station Class IE Power and Protection Systems

All safety systems are designed with provision for periodic testing in conformance with this standard and with Regulatory Guide 1.118. Further discussions on system details may be found in Sections 7.2, 7.3, 7.4, and 7.6.

#### 7.1.2.11.4 IEEE 344—Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations

All safety-related I&C equipment is classified as Seismic Category I and designed to withstand the effects of the safe shutdown earthquake (SSE) and remain functional during normal and accident conditions. Qualification and documentation procedures used for Seismic Category I equipment and systems meet the provisions of IEEE 344 as identified in Section 3.10.

#### 7.1.2.11.5 IEEE 379—Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Class 1E Systems

All safety systems are designed to meet the requirements of IEEE 379 and Regulatory Guide 1.53, which endorses this standard. Further discussion of system details may be found in Sections 7.2, 7.3, 7.4 and 7.6.

#### 7.1.2.11.6 IEEE 384—Standard Criteria for Independence of Class 1E Equipment and Circuits

The safety-related systems described in Sections 7.2, 7.3, 7.4, and 7.6 meet the independence and separation criteria for redundant systems in accordance with IEEE 384. See Subsection 7.1.2.10.5 for conformance to Regulatory Guide 1.75.

### 7.1.2.12 Conformance to Branch Technical Positions

Applicable branch technical positions (BTPs) are identified relative to the I&C systems in Table 7.1-2. The systems are generally designed to conform to the BTP. The degree of conformance, along with any clarifications or exceptions, is discussed in the analysis portions of Sections 7.2 through 7.6.

### 7.1.2.13 Conformance to TMI Action Plan Requirements

TMI action plan requirements are generically addressed in Appendix 1A. Clarifications or exceptions related specifically to I&C (if any) are addressed in the analysis portions of Sections 7.2 through 7.6.

## Table 7.1-1 Comparison of GESSAR II and ABWR I&C Safety Systems

| I & C System | GESSAR II Design | ABWR Design |
|---|---|---|
| General Comparisons for All Safety Systems: | Hard-wired sensor interfaces. | Multiplexed sensor interfaces. |
| | Nuclear system protection system (NSPS) solid-state-based logic and self-test system controllers. | Safety system logic & control (SSLC) microprocessor-based logic and self-test system controllers. |
| Reactor Protection System (RPS): | High scram discharge volume level trip. | Low charging pressure in HCU accumulators trip. |
| | Neutron monitoring system IRM trip. | Neutron monitor SRNM (combined SRM & IRM) trip. |
| | | Added total core flow rapid decrease trip to NMS APRM trip. |
| | Four manual scram switches in two-out-of-four scram arrangement. Manual scram and automatic scram share common trip actuators. | Two manual scram switches in two-out-of-two arrangement backed up by mode switch "SHUTDOWN" position contacts. No trip actuators shared by manual scram and automatic scram function. |
| | Automatic bypass of MSIV closure trip when not in "RUN" mode. | Automatic bypass of MSIV closure trip when not in "RUN" mode and reactor pressure less than 4.14MPa. |
| Emergency Core Cooling System (ECCS): | Div. 1: LPCI + LPCS + ADS<br>Div. 2: LPCI + LPCI + ADS<br>Div. 3: HPCS | Div 1: LPFL + RCIC + ADS<br>Div II: HPCF + LPFL + ADS<br>Div III: HPCF + LPFL |
| | HPCS: Division 3 only (single division & single loop). | HPCF: Divisions II & III (two loops with separate electrical division for each loop). |
| | HPCS: Initiation on Level 2 or high drywell pressure. | HPCF: Initiation on Level 1.5 or high drywell pressure. |
| | HPCS: Logic 1/2 x 2 to start pump, 2/2 to close injection valve. | HPCF. Logic 2/4 to start pump, 2/4 to close injection valve. |
| | ADS: 2/2 (in each of two divisions) actuator signal logic: high drywell pressure and Level 1 and 120 second time delay with Level 3 confirmation. | ADS: 2/4 (in each of two divisions) actuator signal logic: Level 1 and high drywell pressure and 29-second time delay (no Level 3 confirmation signal needed). |
| | RHR/LPCI Mode: 3 pump loops with 2 electrical divisions. | RHR/LPFL Mode: 3 pump loops with 3 electrical divisions. |
| | LPCS: Division 1<br>(RCIC not part of ECCS - initiated by Level 2 only.) | RCIC: Division I - now part of ECCS - initiated by Level 2 or drywell pressure with 2/4 sensor logic channels. |

## Table 7.1-1 Comparison of GESSAR II and ABWR I&C Safety Systems (Continued)

| I & C System | GESSAR II Design | ABWR Design |
|---|---|---|
| Leak Detection and Isolation System (LD&IS): | Leak detection system (LDS) separate from containment and reactor vessel isolation & control system (CRVICS). | Combined LDS and CRVICS to make LD&IS. |
| | Main steam positive leakage & control system (MSPLCS). | MSPLCS deleted. |
| | All inboard isolation valves powered by Division 2; all outboard isolation valves powered by Division 1. | Divisions 1, 2, and 3 are used in various combinations to obtain redundant pairs of inboard/outboard isolation valves. |
| RHR/Wetwell Drywell Spray Mode: | 2 wetwell/drywell cooling divisions. Both automatically and manually actuated. | 2 wetwell/drywell cooling divisions. Manual actuation only. |
| RHR/Suppression Pool Cooling Mode: | 2 loops and 2 divisions. Manual initiation. | 3 loops and 3 divisions. Automatic and manual initiation. |
| Flammability Control System: | Part of combustible gas control system. | Independent system. |
| Standby Gas Treatment System: | Redundant active and passive components. | Redundant active components; single filter train. |
| Emergency Diesel Generator System: | ESF diesels: Divisions 1 & 2. HPCS diesel: Div. 3. | ESF Diesels: Divisions I,II & III (HPCF included on Divisions II & III). |
| Reactor Building Cooling Water: | Open loop to ultimate heat sink. System was called “essential service water system”. | Closed loop with limited quantity of water. |
| Containment Atmospheric Control System: | Hydrogen mixing system interface. | Dedicated hydrogen mixing not required for inerted containment. |
| High Pressure Nitrogen Gas Supply: | (Air supply only) | Replaces air supply to ADS and SRV accumulators. Also used for testing MSIVs. |
| Alternate Rod Insertion (ARI) Function: | (Not applicable) | New function provided by fine motion control rod drive (FMCRD) capability of the rod control & information system (RC&IS). |
| Standby Liquid Control System (SLCS): | Squib-type injection valve. | Motor-operated-type injection valve. |
| | Pump indication “RUN”, “STOP”, “TRIPPED” | Pump indication “RUN”, “STOP” |

## Table 7.1-1 Comparison of GESSAR II and ABWR I&C Safety Systems (Continued)

| I & C System | GESSAR II Design | ABWR Design |
|---|---|---|
| RHR/Shutdown Cooling Mode: | 2 shutdown cooling divisions with 1 suction line. | 3 shutdown cooling divisions with 3 suction lines (1 per division). |
| Remote Shutdown System (RSS): | RCIC controls available at RSS panel | RCIC controls replaced with HPCF controls at RSS panel. |
| Safety Related Display Instrumentation: | Designed to address Regulatory Guide 1.97, Revision 2. | Designed to address Regulatory Guide 1.97, Revision 3. |
| Neutron Monitoring System (NMS): | Class 1E subsystems are IRM, LPRM & APRM. | Class 1E subsystems are SRNM (combines IRM & SRM), LPRM, OPRM & APRM. Added new OPRM function to APRM. |
| | Non-Class 1E subsystems are SRM & TIP, and RBM | Non-Class 1E subsystems are ATIP, and MRBM |
| Process Radiation Monitoring System (PRMS): | — | New system definition and organization, i.e., new instrument groupings, locations and ranges. |
| Drywell Vacuum Relief System: | Electrically operated butterfly valve. | Mechanically operated relief valve. |
| Containment Atmospheric Monitoring System (CAMS) | (Not in GESSAR II scope) | New system provided in ABWR scope. |
| Suppression Pool Temperature Monitoring System: | 4 thermocouples in each of the 4 containment quadrants.<br>4 x 4 = 16 total T/Cs. | 4 thermocouples in each of 4 divisions at 4 of 8 locations.<br>4 x 4 x 4 = 64 total T/Cs.<br>Added suppression pool level monitoring function. |

## Table 7.1-2 Regulatory Requirements Applicability Matrix for I&C Systems

| Applicable Criteria | 10CFR 50.55 | GDC | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 2 | 4 | 10 | 12 | 13 | 15 | 16 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 28 | 29 | 33 | 34 | 35 | 38 | 41 | 44 |
| **Reference Standard (RG, IEEE, ISA)** | 279 | | | | | | | | | | | | | | | | | | | | | | |
| Reactor Protection System | X | X | X | | | X | X | | X | X | X | X | X | X | X | | X | | | | | | |
| Emergency Core Cooling | X | X | X | | | X | X | | X | X | X | X | X | X | | | X | X | X | X | | | |
| Leak Detection & Isolation | X | X | X | | | X | | X | X | X | X | X | X | X | | | X | | X | X | X | X | X |
| RHR/Wetwell Drywell Spray | X | X | X | | | X | | | X | X | X | X | X | X | | | X | | | | X | | X |
| RHR/Supp. Pool Cooling | X | X | X | | | X | | | X | X | X | X | X | X | | | X | | | | X | | X |
| Standby Gas Treatment (Includes GDC 43 and RG 1.52) | X | X | X | | | X | | | X | X | X | X | | X | | | X | | | | | X | |
| Emergency Diesel Support | X | X | X | | | X | | | X | | | | | | | | | | | | | | X |
| Reactor Bldg. Cooling Water | X | X | X | | | X | | | X | X | X | X | X | X | | | X | | X | X | X | | X |
| Essential HVAC Systems | X | X | X | | | X | | | X | X | X | X | X | X | | | X | | | | | | |
| HVAC Emergency Cooling Water | X | X | X | | | X | | | X | X | X | X | X | X | | | X | | | | | | X |
| High Pressure Nitrogen Supply | X | X | X | | | X | | | X | X | X | X | X | X | | | X | | | | | | |

## Table 7.1-2 Regulatory Requirements Applicability Matrix for I&C Systems (Continued)

| Applicable Criteria | 10CFR 50.55 | GDC 2 | 4 | 10 | 12 | 13 | 15 | 16 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 28 | 29 | 33 | 34 | 35 | 38 | 41 | 44 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Reference Standard (RG, IEEE, ISA)** | 279 | | | | | | | | | | | | | | | | | | | | | | |
| Alternate Rod Insertion | | | | | | X | | | X | | | | | | X | | | | | | | | |
| Standby Liquid Control | X | X | X | | | X | | | X | | | | | | | | | | | | | | |
| RHR/Shutdown Cooling | X | | | | | X | X | | X | | | | | | | | | | X | | | | X |
| Remote Shutdown System | X | X | X | | | X | | | X | | | | | | | | | X | X | X | | | X |
| Safety Reactor Display System | | X | X | | | X | | | X | | | | | | | | | | | | | | |
| Neutron Monitoring System | X | X | X | X | X | X | | | X | | | | | | | X | | | | | | | |
| Process Radiation Monitoring | X | X | X | | | X | | X | X | X | X | X | X | X | | X | | | | | | | |
| HP/LP System Interlocks | X | X | X | X | | X | X | | X | | | | | | | | | X | | | | | X |
| Containment Atmospheric Monitoring | X | X | X | | | X | | X | X | | | | | | | | | | | | | X | |
| Suppression Pool Temperature Monitoring | X | X | X | | | X | | X | X | X | X | X | X | X | | | X | | | | X | | |
| Control Systems (Non-Class 1E) | | | | | | X | | | X | | | | | | | | | | | | | | |

## Table 7.1-2 Regulatory Requirements Applicability Matrix for I&C Systems (Continued)

| Applicable Criteria | Regulatory Guide | | | | | | | | BTP | | | | | | II-D | II-E | II-F | | II-K | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1.22 | 1.62 | 1.75 | 1.97 | 1.105 | 1.118 | | 1.151 | 3 | 12 | 20 | 21 | 22 | 26 | 3 | 4.2 | 1 | 3 | 1.23 | 3.13 | 3.15 | 3.18 | 3.21 | 3.22 | 3.23 |
| **Reference Standard (RG, IEEE, ISA)** | 279 | 279 | 384 | | 567.04 | 338 | | 567.02 | 279 | 279 | 279 | RG 1.47 | RG 1.22 | 279 | | | | RG 1.97 | | | | | | | |
| Reactor Protection System | X | X | X | | X | X | | | | X | | X | X | X | | | | | | | | | | | |
| Emergency Core Cooling | X | X | X | | X | X | | | X | | X | X | X | | X | X | | | | X | X | X | X | X | |
| Leak Detection & Isolation | X | X | X | X | X | X | | | | | | X | X | | | X | | X | | | | | | | |
| RHR/Wetwell Drywell Spray | X | X | X | | X | X | | | | | | X | X | | | X | | | | | | | | | |
| RHR/Supp. Pool Cooling | X | X | X | | X | X | | | | | | X | X | | | X | | | | | | | | | |
| Standby Gas Treatment (Includes GDC 43 and RG 1.52) | X | X | X | | X | X | | | | | | X | X | | | | | | | | | | | | |
| Emergency Diesel Support | X | X | X | | | X | | | | | | X | X | | | | | | | | | | | | |
| Reactor Bldg. Cooling Water | X | X | X | | | X | | | | | | X | X | | | | | | | | | | | | |
| Essential HVAC Systems | X | X | X | | | X | | | | | | X | X | | | | | | | | | | | | |
| HVAC Emergency Cooling Water | X | X | X | | | X | | | | | | X | X | | | | | | | | | | | | |
| High Pressure Nitrogen Supply | X | X | X | | | X | | | | | | X | X | | | | | | | | | | | | |

## Table 7.1-2 Regulatory Requirements Applicability Matrix for I&C Systems (Continued)

| Applicable Criteria | Regulatory Guide | | | | | | | | BTP | | | | | | II-D | II-E | II-F | | II-K | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1.22 | 1.62 | 1.75 | 1.97 | 1.105 | 1.118 | | 1.151 | 3 | 12 | 20 | 21 | 22 | 26 | 3 | 4.2 | 1 | 3 | 1.23 | 3.13 | 3.15 | 3.18 | 3.21 | 3.22 | 3.23 |
| **Reference Standard (RG, IEEE, ISA)** | 279 | 279 | 384 | | 567.04 | 338 | | 567.02 | 279 | 279 | 279 | RG 1.47 | RG 1.22 | 279 | | | | RG 1.97 | | | | | | | |
| Alternate Rod Insertion | | | X | | | | | | | | | | | | | | | | | | | | | | |
| Standby Liquid Control | X | X | X | | | X | | | | | | X | X | | | | | | | | | | | | |
| RHR/Shutdown Cooling | X | X | X | | X | X | | | X | | X | X | X | | | | | | | | | | | | |
| Remote Shutdown System | | X | X | | | | | | | | | | | | | | | | | | | | | | |
| Safety Reactor Display System | X | | X | X | X | X | | X | | | | X | X | | X | | X | X | X | | | | | | X |
| Neutron Monitoring System | X | | X | X | X | X | | | | | | X | X | | | | | | | | | | | | |
| Process Radiation Monitoring | X | X | X | X | X | X | | | | | | X | X | | | | | X | | | | | | | |
| HP/LP System Interlocks | X | X | X | | X | X | | | X | | | X | X | | | | | | | | | | | | |
| Containment Atmospheric Monitoring | X | | X | X | X | X | | | | | | X | X | | | | X | X | | | | | | | |
| Suppression Pool Temperature Monitoring | X | | X | X | X | X | | | | | | X | X | | | | X | X | | | | | | | |
| Control Systems (Non-Class 1E) | | | | | | | | X | | | | | | | | | | | | | | | | | |

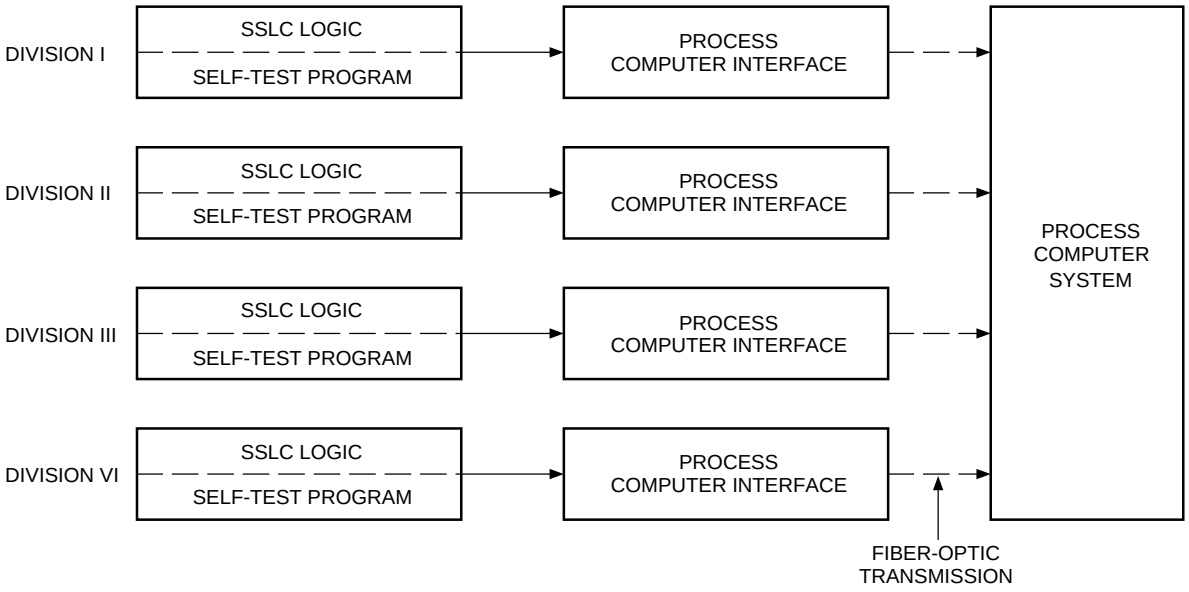
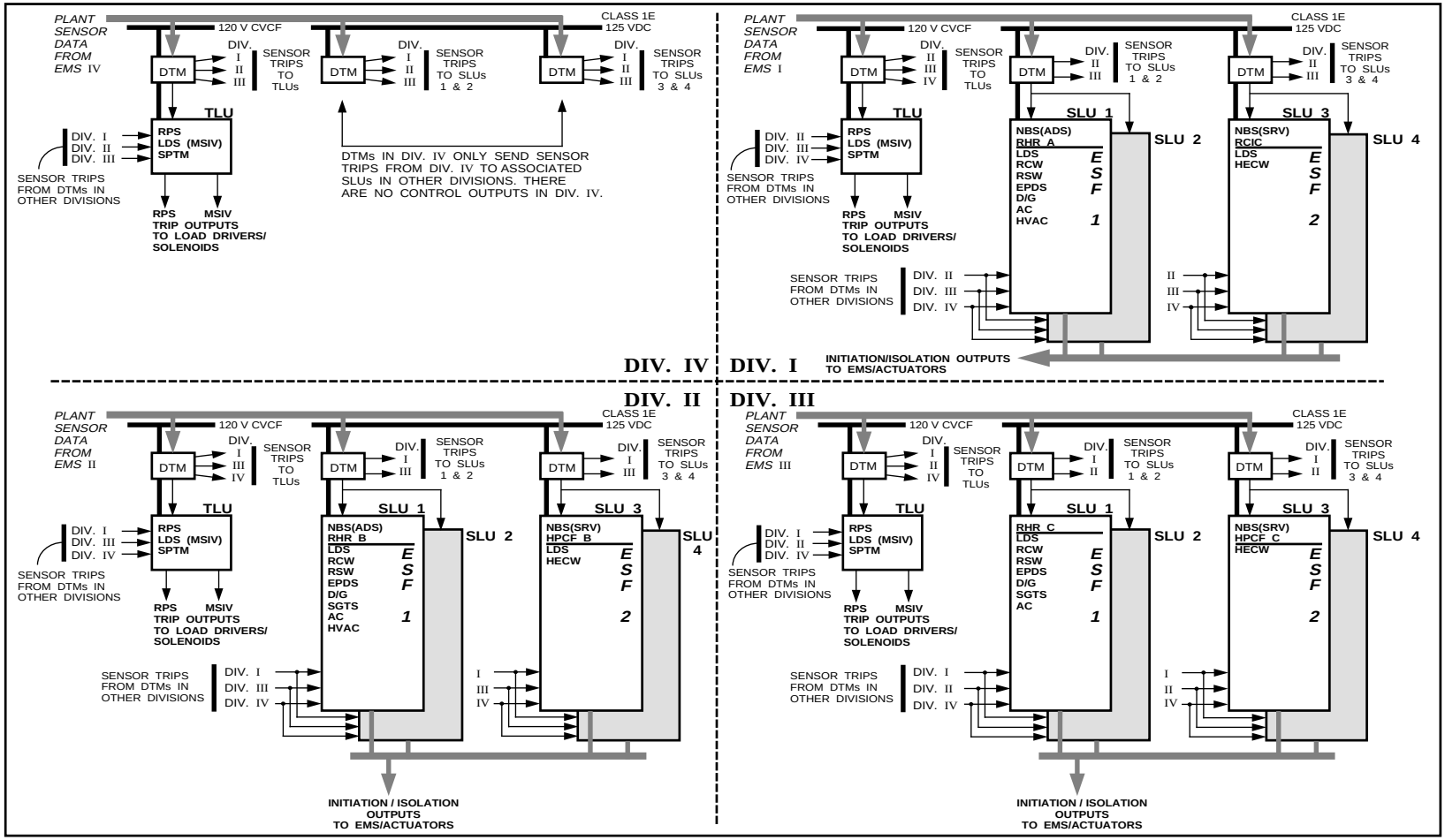



**Figure 7.1-1 SSLC Self-Test System**




**ABBREVIATIONS:**

DTM = DIGITAL TRIP MODULE
EMS = ESSENTIAL MULTIPLEXING SYSTEM
SLU = SAFETY SYSTEM LOGIC UNIT
TLU = TRIP LOGIC UNIT

AC = ATMOSPHERIC CONTROL
D/G = DIESEL GENERATOR
EPDS = ELECTRICAL POWER DISTRIBUTION SYSTEM
ESF = ENGINEERED SAFETY FEATURES
HECW = HVAC EMERGENCY COOLING WATER
HVAC = HEATING, VENTILATING & AIR CONDITIONING
LDS = LEAK DETECTION & ISOLATION SYSTEM
MSIV = MAIN STEAM ISOLATION VALVE
NBS = NUCLEAR BOILER SYSTEM

NMS = NEUTRON MONITORING SYSTEM
PRRM = PROCESS RADIATION MONITORING
RCIC = REACTOR CORE ISOLATION COOLING
RCW = REACTOR BUILDING CLOSED COOLING WATER
RHR = RESIDUAL HEAT REMOVAL
RPS = REACTOR PROTECTION SYSTEM
RSW = REACTOR SERVICE WATER
SGTS = STANDBY GAS TREATMENT SYSTEM
SPTM = SUPPRESSION POOL TEMPERATURE MONITORING

**NOTES:**

1. NMS AND PRRM (NOT SHOWN) ARE STANDALONE SYSTEMS WITH TRIP OUTPUTS TO RPS AND ESF CONTROLLERS OF SSLC.
2. POWER SOURCES (PER DIVISION)
   EMS: CLASS 1E, 125 VDC
   ESF 1/ESF 2: CLASS 1E, 125 VDC
   RPS/MSIV: CLASS 1E, 120 V CVCF
   NMS/PRRM: CLASS 1E, 120 V CVCF

**Figure 7.1-2 Assignment of Interfacing Safety System Logic to SSLC Controllers**

# 7.2 Reactor Protection (Trip) System (RPS)—Instrumentation and Controls

## 7.2.1 Description

### 7.2.1.1 System Description

#### 7.2.1.1.1 RPS Identification

The Reactor Protection System (RPS) is the overall complex of instrument channels, trip logics, trip actuators and scram logic circuitry that initiate rapid insertion of control rods (scram) to shut down the reactor. The RPS also establishes reactor operating modes and provides status and control signals to other systems and annunciators. To accomplish its overall function, the RPS interfaces with the Essential Multiplexing System, Neutron Monitoring System, Process Radiation Monitoring System, Control Rod Drive System, Rod Control and Information System, Reactor Recirculation Control System, Process Computer System, Nuclear Boiler System and other plant systems and equipment. These interfaces are discussed in detail in the following subsections. The RPS IED is provided as Figure 7.2-9. The RPS IBD is provided as Figure 7.2-10.

#### 7.2.1.1.2 RPS Classification

The RPS is classified as Safety Class 2, Seismic Category I, and Quality Group B (electric Safety Class 1E) per Regulatory Guide 1.26 and meets the requirements of 10CFR50.55a(h).

#### 7.2.1.1.3 Power Sources

The RPS utilizes three types of power:

(1) 120 VAC—taken from the four divisional safety system logic and control (SSLC) power supply buses discussed in Section 8.3. Each bus supplies power for one division of RPS logic. Two of the four buses also provide 120 VAC power through the two divisions of RPS scram logic circuitry to the “A” and “B” solenoids of the scram hydraulic control units (HCUs) of the Control Rod Drive System.

(2) 125 VDC—taken from two of the four divisional SSLC battery buses discussed in Section 8.3. Each bus provides 125 VDC power through one of the two divisions of RPS scram logic circuitry to the solenoid of one of the two air header dump valves of the Control Rod Drive System.

SSLC power sources are shown in Figure 7.2-1. Scram and air header dump power distribution is shown in Figure 7.2-8.

#### 7.2.1.1.4 RPS Equipment Design

The RPS is designed to provide reliable single-failure-proof capability to automatically or manually initiate a reactor scram while maintaining protection against unnecessary scrams resulting from single failures. This is accomplished through the combination of fail-safe equipment design and redundant two-out-of-four logic arrangement. All equipment within the RPS is designed to fail into a trip initiating state on loss of power or input signal. In conjunction with this, trip initiating logic signals to and within the RPS are asserted low, whereas trip bypass logic signals and trip bypass permissive logic signals are asserted high.

##### 7.2.1.1.4.1 General RPS Equipment

The RPS equipment is divided into four redundant divisions of sensor (instrument) channels, trip logics and trip actuators, and two divisions of manual scram controls and scram logic circuitry. The sensor channels, divisions of trip logics, divisions of trip actuators and associated portions of the divisions of scram logic circuitry together constitute the RPS scram and air header dump (backup scram) automatic initiation logic. The divisions of manual scram controls and associated portions of the divisions of scram logic circuitry together constitute the RPS scram and air header dump manual initiation logic. The automatic and manual scram initiation logics are independent of each other. RPS equipment arrangement is shown in Figure 7.2-2.

(1) Sensor Channels

Equipment within a sensor channel includes primarily sensors (transducers or switches), multiplexers and digital trip modules (DTMs). The sensors within each channel monitor plant variables (Subsection 7.2.1.1.4.2) send either analog or discrete output to remote multiplexer units (RMUs) within the associated division of Essential Multiplexing System (EMS). Each division of the EMS performs analog-to-digital conversion on analog signals and sends the digital or digitized analog output values of all monitored variables to the DTM within the associated RPS sensor channel. The DTM in each sensor channel compares individual monitored variable values with trip setpoint values and for each variable sends a separate, discrete (trip / no trip) output signal to all four divisions of trip logics.

All equipment within a sensor channel is powered from the same division of Class 1E power source. However, different pieces of equipment may be powered from separate DC power supplies. Within a sensor channel, sensors themselves may belong to the RPS or may be components of another system. Signal conditioning and distribution performed by the RMUs is a function of the EMS and is discussed in Section 7A.2.

(2) Divisions of Trip Logics

Equipment within a division of trip logic includes primarily manual switches, bypass units (BPUs), trip logic units (TLUs) and output logic units (OLUs). The various manual switches provide the operator means to modify the RPS trip logic for special operation, maintenance, testing and reset. The BPUs perform bypass and interlock logic for the channel sensors bypass, main steamline isolation trip special bypass and division trip logic unit bypass. These three bypasses are all manually initiated through individual keylock switches within each of the four divisions. Each BPU sends a separate bypass signal for all four channels to the TLU in the same division for channel sensors bypass and MSL isolation trip special bypass. Each BPU sends the TLU bypass signal to the OLU in the same division.

The TLUs perform automatic scram initiation logic based on reactor operating mode, channel and division trip conditions and bypass conditions. Each TLU receives bistable input signals from the BPU and various switches in the same division and receives isolated bistable inputs from all four sensor channels and divisions of the NMS.

The OLUs perform division trip, seal-in, reset and trip test function. Each OLU receives bypass inputs from the BPU, trip inputs from the TLU and various manual inputs from switches within the same division and provides discrete trip outputs to the trip actuators in the same division. Each OLU also receives an isolated discrete division trip reset permissive signal from equipment associated with one of the two divisions of scram logic circuitry.

All equipment within a division of trip logic is powered from the same division of Class 1E power source. However, different pieces of equipment may be powered from separate DC power supplies, and the BPU, TLU and OLU within a division must be powered from separate DC power supplies.

(3) Divisions of Trip Actuators

Equipment within a division of trip actuators include isolated load drivers and relays for automatic scram and air header dump initiation. Each division of trip actuators receives discrete trip inputs from the OLU in the same division.

The isolated load drivers are fast response time, bistable, solid state, 120 VAC current interrupting devices that can tolerate the high current levels associated with HCU scram solenoids operation. The operation of the load drivers is such that a trip signal (logic “O” voltage level) on the input side will create a high impedance, current interrupting condition on the output side. The load driver outputs are arranged in the scram logic circuitry between the

scram solenoids and scram solenoid 120 VAC power source such that, when in a tripped state, the load drivers will cause de-energization of the scram solenoids (scram initiation). All load drivers within a division interconnect with load drivers in all other divisions into two separate two-out-of-four scram logic arrangements (Figure 7.2-8).

Normally closed relay contacts are arranged in the scram logic circuitry between the air header dump valve solenoids and air header dump valve solenoid 125 VDC power source such that, when in a tripped state (coil de-energized), the relays will cause energization of the air header dump valve solenoids (air header dump initiation). All relays within a division interconnect with relays in all other divisions into two separate two-out-of-four air header dump logic arrangements (Figure 7.2-8).

(4) Divisions of Manual Scram Controls

Equipment within a division of manual scram controls include manual switches, contacts and relays that provide an alternate, diverse, manual means to initiate a scram and air header dump. Each division of manual scram controls interconnects the actuated load power sources to the same division of scram logic circuitry for scram initiation and to both divisions of scram logic circuitry for air header dump initiation.

(5) Divisions of Scram Logic Circuitry

One of the two divisions of scram logic circuitry distributes Div. II 120 VAC power to the A solenoids of all HCUs and Div. II 125 VDC power to the solenoid of one of the two air header dump valves. The other division of scram logic circuitry distributes Div. III 120 VAC power to the B solenoids of all HCUs and Div. III 125 VDC power to the solenoid of the other air header dump valve. The HCUs and air header dump valves themselves are not a part of the RPS.

The arrangement of equipment groups within the RPS from sensors to trip actuators is shown in Figure 7.2-2.

### 7.2.1.1.4.2 Initiating Circuits

The RPS will initiate a reactor scram when any one or more of the following conditions occur or exist within the plant:

(1) NMS monitored conditions exceed acceptable limits

(2) High Reactor Pressure

(3) Low Reactor Water Level (Level 3)

(4) High Drywell Pressure

(5) Main Steamline Isolation

(6) Low Control Rod Drive Charging Header Pressure

(7) High Main Steamline Radiation

(8) Not Used

(9) Turbine Stop Valve Closed

(10) Turbine Control Valve Fast Closure

(11) Operator initiated Manual Scram

(12) High Suppression Pool Temperature

The systems and equipment that provide trip and scram initiating inputs to the RPS for these conditions are discussed in the following subsections. With the exception of the NMS (1) and PRRM (7), and the TB-trips (5 and 7) all of the building signals (9) and (10), all of the other systems provide sensor outputs through the EMS. Analog-to-digital conversion of these sensor output values is done by EMS equipment. NMS and PRRM trip signals are provided directly to the RPS by NMS and PRRM trip logic units. The turbine building signals 9 and 10 are hardwired to connections in the control building. The TB-trips (5 and 7) are provided through hardwired connections.

(1) Neutron Monitoring System (NMS)

Each of the four divisions of the NMS equipment provides separate, isolated, bistable SRNM trip and APRM trip signals to all four divisions of RPS trip logics (Figure 7.2-5).

(a) SRNM Trip Signals

The SRNMs of the NMS provide trip signals to the RPS to cover the range of plant operation from source range through startup range to about 15% of reactor rated power. Three conditions monitored as a function of the NMS comprise the SRNM trip logic output to the RPS. These conditions are upscale, short period and SRNM inoperative. The specific condition within the NMS that caused the SRNM trip output is not detectable within the RPS.

(b) APRM Trip Signals

The APRMs of the NMS provide trip signals to the RPS to cover the range of plant operation from a few percent to greater than reactor rated power. Five conditions monitored as a function of the NMS

comprise the APRM trip logic output to the RPS. These conditions are high neutron flux, high simulated thermal power, APRM inoperative, oscillation power range monitor (ORPM) trip, reactor core flow rapid coastdown. The specific condition within the NMS that caused the APRM trip output is not detectable within the RPS.

(c) OPRM Trip Signals

The OPRM is a functional subsytem of the APRM in each of the four APRM channels. The OPRM trip outputs are combined with other APRM trip signals to produce the final RPS trip signal. The OPRM detects thermal hydraulic instability; its RPS trip function suppresses neutron flux oscillation prior to the violation of safety thermal limits.

(2) Nuclear Boiler System (NBS) (Figure 7.2-6)

(a) Reactor Pressure

Reactor pressure is measured at four physically separated locations by locally mounted pressure transducers. Each transducer is on a separate instrument line and provides analog equivalent output through the EMS to the DTM in one of four RPS sensor channels. The pressure transducers and instrument lines are components of the NBS.

(b) Reactor Water Level

Reactor water level is measured at four physically separated locations by locally mounted level (differential pressure) transducers. Each transducer is on a separate pair of instrument lines and provides analog equivalent output through the EMS to the DTM in one of the four RPS sensor channels. The level transducers and instrument lines are components of the NBS.

(c) Drywell Pressure

Drywell pressure is measured at four physically separated locations by locally mounted pressure transducers. Each transducer is on a separate instrument line and provides analog equivalent output through the EMS to the DTM in one of the four RPS sensor channels of the NBS.

(d) Main Steamline Isolation (Figure 7.2-4)

Each of the four main steamlines can be isolated by closing either the inboard or the outboard isolation valve. Separate position switches on both of the isolation valves of one of the main steamlines provide bistable output through the EMS to the DTM in one of the four RPS sensor channels. Each main steamline is associated with a different RPS

sensor channel. The main steamline isolation valves and position switches are components of the NBS.

(e) High Suppression Pool Temperature

Suppression pool temperature is measured at four physically separated locations by locally mounted sensors. Each sensor is on a separate instrument line and provides analog equivalent of suppression pool temperature to the EMS, which, in turn, provides digitized suppression pool temperature data to the suppression pool monitoring (SPTM) module of SSLC. SSLC, after process and averaging the data, provides trip signal to the corresponding RPS divisional DTM, when the calculated average temperature exceeds the setpoint.

(3) Control Rod Drive (CRD) System (Figure 7.2-6)

(a) CRD Charging Header Pressure

CRD charging header pressure is measured at four physically separated locations by locally mounted pressure transducers. Each transducer is on a separate instrument line and provides analog equivalent output through the EMS to the DTM in one of the four RPS sensor channels. The pressure transducers and instrument lines are components of the CRD System.

(4) Process Radiation Monitoring (PRM) System (Figure 7.2-6)

(a) Main Steamline Radiation

Main steamline radiation is measured by four separate radiation monitors. Each monitor is positioned to measure gamma radiation in all four main steamlines. The PRM System then provides a separate bistable output to the DTM in each of the four RPS sensor channels. The radiation monitors and associated equipment that determine whether or not main steamline radiation is within acceptable limits are components of the PRM System.

(5) Not Used

(6) Reactor Protection System (Figure 7.2-3)

(a) Turbine Stop Valve Closure

Turbine stop valve closure is detected by separate valve stem position switches on each of the four turbine stop valves. Each position switch provides bistable output through hard-wired connections to the DTM in one of the four RPS sensor channels. The turbine stop valves are components of main turbine; however, the position switches are components of the RPS.

(b) Turbine Control Valve Fast Closure

Low hydraulic trip system oil pressure is detected by separate pressure switches on each of the four turbine control valve hydraulic mechanisms. Each pressure switch provides bistable output through hard-wired connections to the DTM in one of the four RPS sensor channels. The turbine control valve hydraulic mechanisms are components of the main turbine; however, the position and pressure switches are components of the RPS.

(c) Manual Scram

Two manual scram switches or the reactor mode switch provide the means to manually initiate a reactor scram independent of conditions within the sensor channels, divisions of trip logics and divisions of trip actuators. Each manual scram switch is associated with one of the two divisions of actuated load power.

In addition to the scram initiating variables monitored by the RPS, one bypass initiating variable is also monitored.

(d) Turbine First-Stage Pressure

Turbine first-stage pressure is measured at four physically separated locations by locally mounted pressure transducers. Each pressure transducer is on a separate instrument line and provides analog equivalent output through the hard-wired connections to the DTM in one of the four sensor channels. Within the RPS divisions of trip logics, this variable forms a bypass component of the turbine stop valve and turbine control valve closure trip logic.

#### 7.2.1.1.4.3 RPS Logic

The combination of division trip, scram, reset and bypass logic that make up the overall RPS logic is shown in Figure 7.2-10. Each division trip logic receives trip inputs from all four sensor channels and NMS divisions and provides a sealed-in trip output to the scram logic when the same trip condition exists in any two or more sensor channels or NMS divisions. At the division trip logic level, various trips and trip initiating conditions can be bypassed as described in the following subsections. The scram logic will initiate a reactor scram when a trip condition exists in any two or more division trip logics. At the scram logic level, no bypasses are possible.

(1) Channel Sensors Bypass

A separate, manual, keylock switch in each of the four divisions provides means to bypass the collective trip outputs of the associated sensor channel. The effect of the channel sensors bypass is to reduce all four division trips to

a coincidence of two out of three tripped sensor channels. Interlocks between the four divisions of trip logic prevent bypass of any two or more sensor channels at the same time. Once a bypass of one sensor channel has been established, bypasses of any of the remaining three sensor channels are inhibited.

A channel sensors bypass in any channel will bypass all trip initiating input signals except those trip signals received from the NMS.

(2) Division Trip Logic Unit Bypass

A separate, manual, keylock switch in each of the four divisions provides means to bypass that division's trip unit output to the scram logic. The effect of the division trip logic bypass is to reduce the scram logic to a coincidence of two out of three tripped divisions. Interlocks between the four division trip logic bypasses prevent bypass of any two or more division trip logics at the same time. Once a bypass of one division of trip logic has been established, bypasses of any of the remaining three division trip logics are inhibited.

(3) MSL Isolation Special Bypass (Figure 7.2-4)

A separate, manual, keylock switch associated with each of the four sensor channels provides means to bypass the MSL isolation trip output signal from the sensor channel to all four divisions of trip logic. This bypass permits continued plant operation while any one MSL is isolated without causing a half scram condition. The effect of the MSL isolation special bypass is to reduce the MSL isolation trip function in all four divisions of trip logic to a coincidence of two out of three sensor channel MSL isolation trips. Interlocks between the four divisions of trip logic prevent MSL isolation special bypass in any sensor channel when either a channel sensors bypass or a MSL isolation special bypass is present in any other sensor channel. Once a MSL isolation special bypass has been established in one sensor channel, the same bypass is inhibited in the other three channels. This bypass is inhibited in all three remaining channels when any channel sensor bypass exists.

(4) Trip Logic and Operating Bypasses

Neutron Monitoring System Trips (Figure 7.2-5)

A coincident NMS trip will occur in each division of trip logic when any two or more out of four divisions of APRM or SRNM trip signals are received from the NMS. The coincident SRNM trip is automatically bypassed when the reactor is in the run mode. The coincident APRM trip cannot be bypassed.

A non-coincident NMS trip will occur in each division of trip logic when any single APRM or SRNM trip signal is received from the NMS. The non-coincident NMS trip is automatically bypassed when the reactor is in the run mode. When the reactor is in the shutdown, refuel or startup mode, the non-coincident NMS trip can be manually bypassed in each division by a separate, manual, keylock non-coincident NMS trip disable switch.

Main Steamline Isolation Trip (Figure 7.2-4)

A MSL isolation trip will occur in each division of trip logic when either the inboard or outboard MSL isolation valve is closed in any two or more unbypassed sensor channels. When the reactor is in the shutdown, refuel or startup mode, the MSL isolation trip function is automatically bypassed in each division of trip logic when reactor pressure in the associated sensor channel is below the bypass setpoint. This bypass permits plant operation when the MSIVs are closed during low power operation.

Low Control Rod Drive (CRD) Charging Header Pressure Trip (Figure 7.2-6)

A low CRD charging header pressure trip will occur in each division of trip logic when CRD charging header pressure is low in any two or more unbypassed sensor channels. This bypass is allowed only whenever the reactor mode switch is either in “Shutdown” or “Refuel” mode position. When the reactor is in the shutdown or refuel mode, the low CRD charging header pressure trip can be manually bypassed in each division of trip logic by separate, manual, keylock CRD charging header pressure trip bypass switches. This bypass allows RPS reset after a scram while CRD charging header pressure is below the trip setpoint. Each division of trip logic sends a separate rod withdraw block signal to the RC&IS when this bypass exists in the division.

Turbine Stop Valve Closed and Turbine Control Valve Fast Closure Trips (Figure 7.2-3)

A turbine stop valve closed trip will occur in each division of trip logic when the turbine stop valve is closed in any two or more unbypassed sensor channels. A turbine control valve fast closure trip will occur in each division of trip logic when either the fast acting solenoid valve is closed or the HTS oil pressure is below the trip setpoint in any two or more unbypassed sensor channels. Both of these trips are automatically bypassed in each division of trip logic when turbine first-stage pressure in the associated sensor channel is below the bypass setpoint. Each division of trip logic sends a separate recirc pump trip initiating signal to the recirc system when these trips occur in the division.

High Reactor Pressure Trip (Figure 7.2-6)

A high reactor pressure trip will occur in each division of trip logic when reactor pressure is above the trip setpoint in any two or more unbypassed sensor channels. There are no operating bypasses associated with this trip function.

Low Reactor Water Level Trip (Figure 7.2-6)

A low reactor water level trip will occur in each division of trip logic when reactor water level is below the trip setpoint in any two or more unbypassed sensor channels. There are no operating bypasses associated with this trip function.

High Drywell Pressure Trip (Figure 7.2-6)

A high drywell pressure trip will occur in each division of trip logic when drywell pressure is above the trip setpoint in any two or more unbypassed sensor channels. There are no operating bypasses associated with this trip function.

High Main Steamline Radiation Trip (Figure 7.2-6)

A high main steamline radiation trip will occur in each division of trip logic when a main steamline radiation trip condition exists in any two or more unbypassed sensor channels. There are no operating bypasses associated with this trip function.

High Suppression Pool Temperature (Figure 7.2-6)

A high suppression pool temperature trip will occur in each division of the trip logic when suppression pool temperature is above the trip setpoint in any two or more unbypassed sensor channels. There are no operating bypasses associated with this trip function.

(5) Manual Scram

A sealed-in manual scram of all HCUs and associated control rods will occur when both manual scram pushbuttons are armed and depressed or when the reactor mode switch is placed in the shutdown position. Depressing only one armed scram pushbutton will result in a sealed-in half scram (de-energization of one division of actuated loads). The scram initiating input received from the mode switch shutdown contacts is automatically bypassed after a sufficient time delay (10 s) to allow for scram seal-in and full insertion of all control rods.

A separate, manual, pushbutton switch in each of the four divisions provides means to manually trip all trip actuators in that division. This sealed-in division manual trip is equivalent to a sealed-in automatic trip from the same division of trip logic. An alternative manual scram can be accomplished by depressing any two or more of the four division manual trip pushbuttons.

(6) Reset Logic

A single, manual, three-position, toggle switch provides means to reset the manual scram seal-in circuitry in both divisions of manual scram controls. If either of the manual scram pushbuttons is still depressed when a reset is attempted, the reset will not have any effect.

A separate, manual, pushbutton associated with each division of trip actuators provides means to reset the seal-in at the input of all trip actuators in the same division. If the conditions that caused the division trip have not cleared when a reset is attempted, the reset will not have any effect. After a single division trip, reset is possible immediately; however, if a full scram has occurred, reset is inhibited for 10 seconds to allow sufficient time for scram completion.

As a consequence of a full scram, the CRD charging header pressure will drop below the trip setpoint, resulting in a trip initiating input to all four divisions of trip logic. While this condition exists, reset of the manual scram circuitry is possible; however, the four divisions of trip logic cannot be reset until the CRD charging pressure trip is manually bypassed in all four divisions and all other trip initiating conditions have cleared.

### 7.2.1.1.4.4 Redundancy and Diversity

Instrument sensing lines from the reactor vessel are routed through the drywell and terminate outside the primary containment. Instruments mounted on instrument racks in the four quadrants of the Reactor Building sense reactor vessel pressure and water level from this piping. Valve position switches are mounted on valves from which position information is required. The sensors for RPS signals from equipment in the Turbine Building are mounted locally. The four battery-powered inverters and divisional 120 VAC power suppliers for the SSLC and RPS are located in an area where they can be serviced during reactor operation. Sensor signals (via the multiplex network) and power cables are routed to four SSLC cabinets (in which RPS components are located) in the divisional electrical compartments. One logic cabinet is used for each division.

The redundancy portions of the RPS have physically separated sensor taps, sensing lines, sensors, sensor rack locations, cable routing, and termination in four separate panels in the control room. By the use of four or more separate redundant sensors for

each RPS variable with separate redundant logic and wiring, the RPS has been protected from a credible single failure. For additional information on redundancy of RPS subsystems, refer to Subsection 7.2.1.1.4.2. For information on the protection provided within SSLC and RPS against common-mode failure of the redundant channels, refer to Appendix 7C.

Redundancy of the RPS logic power supply is provided. There are four Class 1E uninterruptible power sources which supply electrical power, one to each division of the RPS. A loss of one power supply will neither inhibit protective action nor cause a scram.

### 7.2.1.1.4.5 Actuated Devices

The devices actuated by the RPS trip and scram logic include the 120 VAC powered A and B scram solenoids of the HCUs and the 125 VDC powered air header dump valves. The A solenoids of the HCUs are energized by one division of power and the B solenoids by another division of power. When any single RPS division is in a tripped state or when only one of the manual scram pushbuttons is depressed, all of either the A or the B solenoids will be de-energized, resulting in a half-scram condition. A full scram of the pair of control rods associated with a particular HCU will occur when both the A and B solenoid of the HCU are de-energized. The HCUs and associated control rod pairs are divided into four groups. The RPS supplies power to each group from separate RPS power distribution circuits. The combination of control rods within each group is such that hot shutdown can be achieved even in the event of failure to scram of an entire rod group.

The solenoid of one of the air header dump valves is energized by one division of power and the solenoid of the other air header dump valve is energized by another division of power. When the solenoid of either of the air header dump valves is energized, the air header will be released, resulting in insertion of all control rods. The arrangement of RPS power distribution circuits and actuated devices is shown in Figure 7.2-1.

### 7.2.1.1.4.6 Separation

Four independent sensor channels monitor the various process variables listed in Subsection 7.2.1.1.4.2. The redundant sensor devices are separated so that no single failure can prevent a scram. The arrangement of RPS sensors mounted in local racks is shown in Figure 7.2-2. Locations for local RPS racks and panels are shown on the instrument location drawings provided in Section 1.7. Divisional separation is also applied to the Essential Multiplexing System (EMS), which provides data highways for the sensor input to the logic units. Physically separated cabinets are provided for the four scram logics. Fiber-optic cable routing from remote multiplexing units (RMUs) to control room equipment is shown in raceway plans provided by reference in Section 1.7. The criteria for separation of sensing lines and sensors are discussed in Section 7.1.

The mode switch, low CRD accumulator charging pressure trip and other selected bypass switches scram reset switches and manual scram switches are all mounted on the principal control console. Each device is mounted in a metal enclosure and has a sufficient number of barrier devices to maintain adequate separation between redundant portions of the RPS.

The outputs from the logic cabinets to the scram pilot solenoids are run in separate rigid conduits with no other wiring. The four wire ways match the four scram groups shown in Figure 7.2-8. The groups are selected so that the failure of one group to scram will not prevent a reactor shutdown. The scram group conduits have unique identification and are separately routed as Division II and III conduits for the A and B solenoids of the scram pilot valves, respectively. This corresponds to the divisional assignment of their power sources.

Signals which must run between redundant RPS divisions are electrically / physically isolated by isolators to provide separation.

RPS inputs to annunciators, recorders, and the computer are arranged so that no malfunction of the annunciating, recording, or computing equipment can functionally disable the RPS. Direct signals from RPS sensors are not used as inputs to annunciating or data-logging equipment. Electrical isolation is provided between the primary signal and the information output by fiber-optic cable interfaces.

#### 7.2.1.1.5 Environmental Considerations

Electrical equipment for the RPS is located in the drywell, control structure, containment, and in the Turbine Building. The environmental conditions for these areas are shown in Section 3.11.

#### 7.2.1.1.6 Operational Considerations

##### 7.2.1.1.6.1 Reactor Operator Information

(1) Indicators

Scram group indicators extinguish when an actuator logic prevents output current from the 120 VAC power source to the scram pilot valve solenoid associated with the actuator logic.

Recorders (which are not part of the RPS) in the main control room also provide information regarding reactor vessel water level, and reactor power level.

(2) Annunciators

Each RPS trip channel input is provided to the Containment Cooling System (CCS) annunciator system through isolation devices. Trip logic trips, manual trips, and certain bypasses also signal the annunciator system.

All RPS instrument channel trips shall initiate an annunciation of the variable, causing the trip in the control room to alert the plant operator of a trip condition. The final output trips for each RPS division shall have separate single annunciation of the tripped condition of each RPS division. All bypassed RPS instrument channels or division logics whose bypassed condition is not a normal condition of operation shall also be annunciated. As an annunciator system input, a channel trip also sounds an audible alarm which can be silenced by the operator. The annunciator window lights latch in until reset manually. Reset is not possible until the condition causing the trip has been cleared.

(3) Computer Alarms

A computer printout identifies each tripped channel; however, status indication at the RPS trip channel device may also be used to identify the individual sensor that tripped in a group of sensors monitoring the same variable.

Upon detection of a status change of any of the preselected sequential events contacts, the sequence-of-events log shall be initiated and shall signal the beginning of an event. This log will include both NSSS and BOP inputs. Changes of state received 5 milliseconds or more apart are sequentially differentiated on the printed log, together with time of occurrence, which shall be printed in hours, minutes, seconds, and milliseconds. Use of the alarm typewriter and computer is not required for plant safety. The printout of trips is particularly useful in routinely verifying the correct operation of pressure, level, and valve position switches as trip points are passed during startup, shutdown, and maintenance operations.

#### 7.2.1.1.6.2 Reactor Operator Controls—Mode Switch

A conveniently-located, multiposition, keylock mode switch is provided to select the necessary scram functions for various plant conditions. The mode switch selects the appropriate sensors for scram functions and provides appropriate bypasses. The switch also interlocks such functions as control rod blocks and refueling equipment permissives which are not considered as part of the RPS. The switch is designed to provide separation between signals to the four trip logic divisions. The mode switch positions and their related functions are as follows:

(1) SHUTDOWN

— Initiates a reactor scram

— Selects lower NMS neutron flux trip setpoint

— Enables NMS SRNM trips

— Enables manual selection of non-coincident NMS trip function

— Enables manual CRD charging pressure trip bypass and automatically bypasses the following trip functions:

(a) Turbine control valve fast closure trip

(b) Turbine stop valve closure trip

(c) MSIV closure trip if reactor pressure is below bypass setpoint

(2) REFUEL

— Enables same trip bypasses and NMS trip functions as shutdown mode.

(3) STARTUP

— Enables same trip and bypass functions as REFUEL mode except when CRD charging pressure trip bypass is disabled.

(4) RUN

— Disables all trip bypasses enabled by any of the other three modes.

— Disables SRNM trip and non-coincident NMS trip and deselects lower NMS neutron flux trip setpoint.

Mode switch position is also provided for use by other systems, including NMS, RC&IS and LDS.

#### 7.2.1.1.7 Setpoints

Instrument ranges are chosen to cover the range of expected conditions for the variable being monitored. Additionally, the range is chosen to provide the necessary accuracy for any required setpoints and to meet the overall accuracy requirements of the channel.

(1) Neutron Monitoring System Trip

To protect the fuel against high heat generation rates, neutron flux is monitored and used to initiate a reactor scram. The Neutron Monitoring System is discussed in Section 7.6.

(2) Reactor Vessel System High Pressure

Excessively high pressure within the reactor vessel threatens to rupture the reactor coolant pressure boundary. A reactor vessel pressure increase during reactor operation compresses the steam voids and results in a positive reactivity insertion. This causes increased core heat generation that could lead to fuel failure and system overpressurization. A scram counteracts a pressure increase by quickly reducing core fission-heat generation. The reactor vessel high-pressure scram setting is chosen slightly above the reactor vessel maximum normal operation pressure to permit normal operation without spurious scram yet provide a wide margin to the maximum allowable reactor vessel pressure. The location of the pressure measurement, as compared to the location of highest nuclear system pressure during transients, was also considered in the selection of the high-pressure scram setting. The reactor vessel high-pressure scram works in conjunction with the pressure-relief system to prevent reactor vessel pressure from exceeding the maximum allowable pressure. The reactor vessel high-pressure scram setting also protects the core from exceeding thermal hydraulic limits that result from pressure increases during events that occur when the reactor is operating below rated power and flow.

(3) Reactor Vessel Low Water Level

Low water level in the reactor vessel indicates that the reactor is in danger of being inadequately cooled. Should water level decrease too far, fuel damage could result as steam forms around fuel rods. A reactor scram protects the fuel by reducing the fission-heat generation within the core. The reactor vessel low water level scram setting was selected to prevent fuel damage following abnormal operational transients caused by single equipment malfunctions or single operator errors that result in a decreasing reactor vessel water level. The scram setting is far enough below normal operational levels to avoid spurious scrams. The setting is high enough above the top of the active fuel to assure that enough water is available to account for evaporation loss and displacement of coolant following the most severe abnormal operation transient involving a level decrease.

(4) Turbine Stop Valve Closure

Closure of the turbine stop valve with the reactor at power can result in a significant addition of positive reactivity to the core as the reactor vessel pressure rise causes steam voids to collapse. The turbine stop valve closure scram initiates a scram earlier than either the Neutron Monitoring System or reactor vessel high pressure. The scram counteracts the addition of positive reactivity caused by increasing pressure by inserting negative reactivity with

control rods. Although the reactor vessel high-pressure scram, in conjunction with the pressure relief system, is adequate to preclude over-pressurizing the nuclear system, the turbine stop valve closure scram provides additional margin to the reactor vessel pressure limit. The turbine stop valve closure scram setting provides the earliest positive indication of valve closure.

(5) Turbine Control Valve Fast-Closure

With the reactor and turbine generator at power, fast closure of the turbine control valves can result in a significant addition of positive reactivity to the core as nuclear system pressure rises. The turbine control valve fast-closure scram initiates a scram earlier than either the neutron monitoring system or nuclear system high pressure. The scram counteracts the addition of positive reactivity resulting from increasing pressure by inserting negative reactivity with control rods. Although the nuclear system high-pressure scram, in conjunction with the pressure relief system, is adequate to preclude over-pressurizing the nuclear system, the turbine control valve fast-closure scram provides additional margin to the nuclear system pressure limit. The turbine control valve fast-closure scram setting is selected to provide timely indication of control valve fast closure.

(6) Main Steamline Isolation

The main steamline isolation valve closure can result in a significant addition of positive reactivity to the core as nuclear system pressure rises. The main steamline isolation scram setting is selected to give the earliest positive indication of main steamline isolation without inducing spurious scrams.

(7) Low Charging Pressure to Control Rod Drive Hydraulic Control Unit Accumulators

The CRD Hydraulic System normally supplies charging water at sufficient pressure to charge all scram accumulators of the individual control rod HCUs to pressure values that will assure adequate control rod scram insertion rates during a full reactor trip or scram. A low charging water pressure is indicative of the potential inability to maintain the scram accumulators pressurized. A reactor trip is initiated after a specified time delay, before the charging water pressure drops to a value that could eventually result in slower than normal scram speed control rod insertion.

(8) Drywell High Pressure

High pressure inside the drywell may indicate a break in the reactor coolant pressure boundary. It is prudent to scram the reactor in such a situation to

minimize the possibility of fuel damage and to reduce energy transfer from the core to the coolant. The drywell high-pressure scram setting is selected to be as low as possible without inducing spurious scrams.

(9) Main Steamline High Radiation

High radiation in the vicinity of the main steamlines may indicate a gross fuel failure in the core. When high radiation is detected near the steamlines, a scram is initiated to limit release of fission products from the fuel. The high radiation trip setting is selected high enough above background radiation levels to avoid spurious scrams yet low enough to promptly detect a gross release of fission products from the fuel. More information on the trip setting is available in Section 7.3.

(10) High Suppression Pool Temperature

Automatic reactor scram shall be initiated when the condition of high suppression pool temperature is sensed. This is disclosed in the high suppression pool temperature monitoring system in Subsection 7.2.1.1.4.2(2)(e).

### 7.2.1.1.8 Containment Electrical Penetration Assignment

Electrical containment penetrations are assigned to the protection systems on a four-division basis (Subsections 7.2.1.1.4.1 and 4.6).

Each penetration is provided with a NEMA-4 enclosure box on each end, providing continuation of the metal wire ways (Subsection 7.2.1.1.4.6).

### 7.2.1.1.9 Cable Spreading Area Description

The cable spreading areas adjacent to the control room are termed cable rooms and electrical equipment rooms. A description of the separation criteria used in these rooms is in Section 8.3.

### 7.2.1.1.10 Main Control Room Area

Virtually all hardware within the RPS design scope is located within the four separate and redundant safety system logic and control (SSLC) cabinets in the main control room, except the instrumentation for monitoring turbine stop valve closure and turbine control valve fast closure, and turbine first-stage pressure. The panels are mounted on four separate control complex system steel floor sections which, in turn, are installed in the main control room. The major control switches are located on the principal console.

#### 7.2.1.1.11 Control Room Cabinets and Their Contents

The SSLC logic cabinets, which contain the RPS for Divisions I, II, III, and IV, include a vertical board for each division. The vertical boards contain digital and solid-state discrete and integrated circuits used to condition signals transferred to the SSLC from the EMS. They also contain combinational and sequential logic circuits for the initiation of safety actions and/or alarm annunciation, isolators for electrical and physical separation of circuits used to transmit signals between redundant safety systems or between safety and non-safety systems, and system support circuits such as power supplies, automatic testing circuits, etc. Load drivers with solid-state switching outputs for actuation solenoids, motor control centers, or switchgear may be located in the control room.

The principal console contains the reactor mode switch, the RPS manual scram push-button switches, the CRD scram reset switches and the bypass switches for the low CRD accumulator charging pressure.

#### 7.2.1.1.12 Test Methods That Enhance RPS Reliability

Surveillance testing is performed periodically on the RPS during operation. This testing includes sensor calibration, response-time testing, trip channel actuation, and trip time measurement with simulated inputs to individual trip modules and sensors. The sensor channels can be checked during operation by comparison of the associated control room displays on other channels of the same variable. Fault-detection diagnostic testing is not being used to satisfy Technical Specification requirements for surveillance.

#### 7.2.1.1.13 Interlock Circuits to Inhibit Rod Motion

Interlocks between the RPS and RC&IS inhibit rod withdrawal when the CRD accumulator charging pressure trip bypass switch is in the BYPASS position. These interlocks assure that no rods can be withdrawn when conditions are such that the RPS cannot reinsert rods if necessary.

#### 7.2.1.1.14 Support Cooling System and HVAC Systems Descriptions

The cooling (ventilating) systems important for proper operation of RPS equipment are described in Section 9.4.

### 7.2.1.2 Design Bases

Design bases information requested by IEEE-279 is discussed in the following paragraphs. These IEEE-279 design bases aspects are considered separately from those more broad and detailed design bases for this system cited in Subsection 7.1.2.2.

(1) Conditions

Generating station conditions requiring RPS protective actions are defined in Chapter 16 (Technical Specifications).

(2) Variables

The generating station variables which are monitored cover the protective action conditions that are identified in Subsection 7.2.1.1.4.2.

(3) Sensors

A minimum number of LPRMs per APRM are required to provide adequate protective action. This is the only variable that has spatial dependence (IEEE-279, Paragraph 3.3).

(4) Operational Limits

Operational limits for each safety-related variable trip setting are selected with sufficient margin to avoid a spurious scram. It is then verified by analysis that the release of radioactive material following postulated gross failure of the fuel or the reactor coolant pressure boundary is kept within acceptable bounds. Design basis operational limits in Chapter 16 are based on operating experience and constrained by the safety design basis and the safety analyses.

(5) Margin Between Operational Limits

The margin between operational limits and the limiting conditions of operation (scram) for the Reactor Protection System are described in Chapter 16. The margin includes the maximum allowable accuracy error, sensor response times, and sensor setpoint drift.

(6) Levels Requiring Protective Action

Levels requiring protective action are provided in Chapter 16. These levels are design basis setpoints and are at least as limiting as the limiting safety system settings provided in Chapter 16.

(7) Ranges of Energy Supply and Environmental Conditions

The RPS 120 VAC power is provided by the four battery-powered inverters, for the SSLC, each with an alternate Class 1E 120 VAC supply. The batteries, which are designed for a two-hour minimum capacity, have sufficient stored energy to ride through switching transients in the switch yards in order to prevent switching transients from causing a scram. The alternate sources of 120V power are provided to each SSLC bus from transformers powered from the 6.9 kV emergency diesel generators. Since there are three diesel

generators, the fourth division alternate power originates from the first division diesel.

Environmental conditions for proper operation of the RPS components are covered in Section 3.11 for inside and outside the containment.

(8) Unusual Events

Unusual events are defined as malfunctions or accidents and other events which could cause damage to safety systems. Chapter 15 (Accident Analyses) describes the following credible accidents and events: floods, storms, tornados, earthquakes, fires, LOCA, pipe break outside the containment, and feedwater line break. A discussion of each of these events, as applicable to the subsystems of the RPS, follows:

(a) Floods

The buildings containing RPS 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; therefore, none of the RPS functions are affected by flooding. Internal flooding sources are covered in Section 3.4.

(b) Storms and Tornados

The buildings containing RPS components have been designed to withstand all credible meteorological events and tornados as described in Section 3.3. Superficial damage may occur to miscellaneous station property during a postulated tornado but this will not impair the RPS capabilities.

(c) Earthquakes

The structures containing RPS components, except the turbine building, have been seismically qualified (Sections 3.7 and 3.8) and will remain functional during and following a safe shutdown earthquake (SSE). Since reactor high pressure and power trips are diverse to the turbine scram variables, locating these sensors in the turbine enclosure does not compromise the ability of the RPS to provide protective action when required.

(d) Fires

To protect the RPS in the event of a postulated fire, the RPS trip logics are contained within the four separate independent SSLC cabinets. The separation of the cabinets and their individual steel construction assures

that the RPS functions will not be prevented by a postulated fire within any of the divisional panels. Incombustible or fire retardant materials are used as much as possible. The use of separation and fire barriers ensures that even though some portion of the system may be affected, the RPS will continue to provide the required protective action (Section 9.5).

(e) LOCA

The following subsystem components are located inside the drywell and would be subjected to the effects of a design basis LOCA:

(i) Neutron Monitoring System (NMS) cabling from the detectors to the main control room

(ii) MSIV Inboard Position Sensors

(iii) Reactor vessel pressure and reactor vessel water level instrument taps and sensing lines which terminate outside the drywell; and drywell pressure taps

These items have been environmentally qualified to remain functional during and following a LOCA as discussed in Section 3.11.

(f) Pipe Break Outside Containment

This condition will not affect the reliability of the RPS.

(g) Feedwater Break

This condition will not affect the RPS.

(h) Missiles

Missile protection is described in Section 3.5.

(9) Performance Requirements

The minimum performance requirements are provided in Chapter 16.

A logic combination (two out of four) of instrument channel trips actuated by abnormal or accident conditions will initiate a scram and produce independent logic seal-ins within each of the four logic divisions. The trip conditions will be annunciated and recorded on the process computer. The trip seal-in will maintain a scram signal condition at the CRD System terminals until the trip channels have returned to their normal operating range and the seal-in is manually reset by operator action. Thus, once a trip signal is present long enough to initiate a scram and the seal-ins, the protective action will go to completion.

## 7.2.2 Conformance Analysis

This subsection presents an analysis of how the various functional requirements and the specific regulatory requirements of the RPS design bases are satisfied.

### 7.2.2.1 Conformance to Design Bases Requirements

(Statements of the Design Bases Are Given in Section 7.1.2.2.)

(1) Design Bases 7.1.2.2(1)(a)

The RPS is designed to provide timely protection against the onset and consequences of conditions that threaten the integrity of the fuel barrier. Chapter 15 identifies and evaluates events that jeopardize the fuel barrier. The methods of assessing barrier damage and radioactive material releases, along with the methods by which abnormal events are sought and identified, are presented in that chapter.

Design bases require that the precision and reliability of the initiation of reactor scrams be sufficient to prevent or limit fuel damage.

Table 7.2-1 provides a listing of the sensors selected to initiate reactor scrams and delineates the range for each sensor. Setpoints, accuracy and response time can be found in Chapter 16. This information establishes the precision of the RPS variable sensors.

The selection of scram trip settings has been developed through analytical modeling, historical use of initial setpoints and adoption of new variables and setpoints as experience was gained. The initial setpoint selection method provided for settings which were sufficiently above the normal operating levels (to preclude the possibilities of spurious scrams or difficulties in operation) but low enough to protect the fuel. As additional information became available or systems were changed, additional scram variables were provided using the above method for initial setpoint selection. The selected scram settings are analyzed to verify that they are conservative and that the fuel and fuel barriers are adequately protected. In all cases, the specific scram trip point selected is a conservative value that prevents damage to the fuel taking into consideration previous operating experience and the analytical models.

(2) Design Basis 7.1.2.2.(1)(b)

The scram initiated by reactor high pressure, in conjunction with the pressure relief system, is sufficient to prevent damage to the reactor coolant pressure boundary as a result of internal pressure. The MSIV closure scram provides a greater margin to the RCPB pressure safety limit than does the high pressure

scram. For turbine generator trips, the stop valve closure scram and turbine control valve fast closure scram provide a greater margin to the nuclear system pressure safety limit than does the high pressure scram. Chapter 15 identifies and evaluates accidents and abnormal operational events that result in nuclear system pressure increases. In no case does pressure exceed the RCPB safety limit.

(3) Design Basis 7.1.2.2(1)(c)

The scram initiated by the main steamline radiation monitoring system and reactor vessel low-water level satisfactorily limits the radiological consequences of gross failure of the fuel or RCPB. (Chapter 15 evaluates gross failure of the fuel and RCPB). In no case does the release of radioactive material to the environs result in exposures which exceed the guidelines of applicable published regulations.

(4) Design Basis 7.1.2.2(1)(d)

Scrams are initiated by variables which are designed to indirectly monitor fuel temperature and protect the reactor coolant pressure boundary. The Neutron Monitoring System monitors fuel temperature indirectly using incore detectors. The incore detectors monitor the reactor power level by detecting the neutron level in the core. Reactor power level is directly proportional to neutron level and the heat generated in the fuel. Although the NMS does not monitor fuel temperature directly by establishing a correlation between fuel temperature and reactor power level, scram setpoints can be determined for protective action which will prevent fuel damage.

The RCPB is protected by monitoring parameters which indicate reactor pressure directly or anticipate reactor pressure increases. Reactor pressure is monitored directly by pressure sensors which are connected directly to the reactor pressure vessel through sensing lines and pressure taps. In addition, reactor pressure transients are anticipated by monitoring the closure of valves which shut off the flow of steam from the reactor pressure vessel and cause rapid pressure increases. The variables monitored to anticipate pressure transients are MSIV position, turbine stop valve closure, and turbine control valve fast closure. If any of these valves were to close, pressure would rise very rapidly; therefore, this condition is anticipated and a trip is initiated to minimize the pressure transient occurring.

Chapter 15 identifies and evaluates those conditions which threaten fuel and RCPB integrity. In no case does the core exceed a safety limit.

(5) Design Basis 7.1.2.2(1)(e)

The scrams initiated by the NMS drywell pressure, reactor vessel pressure, high suppression pool temperature, reactor vessel water level, turbine stop valve closure, MSIV bypass, and turbine control valve fast closure will prevent fuel damage. The scram setpoints and response time requirements for these variables are identified in Chapter 16 and have been designed to cover the expected range of magnitude and rates of change during abnormal operational transients without fuel damage. Chapter 15 identifies and evaluates those conditions which threaten fuel integrity. With the selected variables and scram setpoints, adequate core margins are maintained relative to thermal/hydraulic safety limits.

(6) Design Basis 7.1.2.2(1)(f)

Neutron flux is the only essential variable of significant spatial dependence that provides inputs to the Reactor Protection System(RPS). The basis for the number and locations follows. The other requirements are fulfilled through the combination of logic arrangement, channel redundancy, wiring scheme, physical isolation, power supply redundancy, and component environmental capabilities.

Two transient analyses are used to determine the minimum number and physical location of required LPRMs for each APRM.

(a) The first analysis is performed with operating conditions of 100% reactor power and 100% recirculation flow using a continuous rod withdrawal of the maximum worth control rod. In analysis, LPRM detectors are mathematically removed from the APRM channels. This process is continued until the minimum numbers and locations of detectors needed to provide protective action are determined for this condition.

(b) The second analysis is performed with operating conditions of 100% reactor power and 100% recirculation flow using a reduction of recirculation flow at a fixed design rate. LPRM detectors are mathematically removed from the APRM channels. This process is continued until the minimum numbers and locations of detectors needed to provide protective action are determined for this condition.

The results of the two analyses are analyzed and compared to establish the actual minimum number and location of LPRMs needed for each APRM channel.

(7) RPS Design Basis 7.1.2.2.1(1)(g) through (n)

Sensors, channels, and logics of the RPS are not used directly for automatic control of process systems. An isolated NMS signal is used with the recirculation flow control system (Section 7.7); therefore, failure in the controls and instrumentation of process systems cannot induce failure of any portion of the protection system.

Failure of any RPS power supply would result in de-energizing one of the two scram valve pilot solenoids on each scram valve. Alternate power is available to the RPS buses. A complete sustained loss of electrical power to two or more power supplies would result in a scram.

The RPS is designed so that it is only necessary for trip variables to exceed their trip setpoints for sufficient length of time to trip the digital trip modules and seal-in the associated trip logic. Once this is accomplished, the scram will go to completion regardless of the state of the variable which initiated the protective action.

When the initiating condition has cleared and a sufficient (10 seconds) time delay has occurred, the scram may be reset only by operator actuation of the scram reset switches in the main control room.

RPS cabling is routed in separate raceways or conduits for each division for all wiring for sensors, racks, panels, and scram solenoids.

Physical separation and electrical isolation between redundant portions of the RPS is provided by separated process instrumentation, separated racks, and either separated or protected panels and cabling.

Separate panels are provided for each division except for the control room principal console, which has internal metal barriers. Where equipment from more than one division is in a panel, divisional separation is provided by fire barriers and/or physical distance of 15.2 cm or more where practicable. Where wiring must be run between redundant divisions, divisional separation is provided by electronic optical isolators or by fiber optic cables.

The ability of the RPS to withstand a safe shutdown earthquake is discussed in Subsection 7.2.1.2.

The ability of the RPS to function properly with a single failure is discussed in Subsection 7.2.1.2.

The ability of the RPS to function properly while any one sensor or channel is bypassed or undergoing test or maintenance is discussed in Subsection 7.2.1.2.

The RPS logic circuit is designed so that an automatic scram will be initiated when the required number of sensors for any monitored variable exceeds the scram setpoint.

Separate racks are provided for the RPS instrumentation for each division and are installed in different locations.

(8) Design Basis 7.1.2.2(1)(o) and (p)

Access to trip settings, component calibration controls, test points, and other terminal points is under the control of plant operations supervisory personnel.

Manual bypass of I&C equipment components is under the control of the operator in the control room. If the ability to trip some essential part of the system is bypassed, this fact is continuously annunciated in the control room. Operating bypasses are removed by normal reactor operation and need not be annunciated.

For the subsystem operational bypasses (Subsection 7.2.1), bypassing of these subsystem components provides a continuous annunciation in the control room. If other components are bypassed, such as taking a sensor out of service for calibration or testing, this condition will also be annunciated continuously in the control room through the administratively controlled manual actuation of the RPS out-of-service annunciator associated with that sensor.

#### 7.2.2.1.1 Other Design Basis Requirements

The environment in which the instruments and equipment of the Reactor Protection System must operate is given in Section 3.11.

The control room maximum environment is predicated on supplying the control room with minimum outside air for recirculated conditioned air. The minimum environment is predicated on a mixture of outside and recirculated air concurrent with minimum equipment heat loss. Components that monitor RPS trip initiating conditions that must function in the environment resulting from a RCPB break inside the drywell include, (1) are the condensing chambers, (2) inboard MSIV position switches, (3) NMS cabling, (4) reactor vessel pressure taps, (5) reactor vessel water level instrument taps, (6) sensing lines, and (7)drywell pressure taps. Special precautions are taken to ensure their operability after the accident. The condensing chambers and all essential components of the control and electrical equipment are either similar to those that have successfully undergone qualification testing in connection with other projects or additional qualification testing under simulated environmental conditions has been conducted.

The number of operable channels for the essential monitored variables is given in Table 7.2-2. The minimums apply to any untripped trip system. A tripped trip system may have any number of inoperative channels. Because reactor protection requirements vary with the mode in which the reactor operates, the table shows different functional requirements for the RUN and STARTUP modes. These are the only modes where more than one control rod can be withdrawn from the fully inserted position.

In case of a loss-of-coolant accident, reactor shutdown occurs immediately following the accident as process variables exceed their specified setpoint. Operator verification that shutdown has occurred may be made by observing one or more of the following indications:

(1) Control rod status lamps indicating each rod fully inserted.

(2) Control rod scram valve status lamps indicating open valves.

(3) Neutron monitoring channels and recorders indicating decreasing neutron flux.

Following generator load rejection, a number of events occur in the following chronological order:

(4) The pressure in the hydraulic oil lines to the control valves drops and pressure sensors signal the RPS to scram. At the same time, the turbine logic pressure controller initiates fast opening of the turbine bypass valves to minimize the pressure transient. Turbine stop valve closure and turbine control valve fast closure initiates the recirculation pump trip (RPT) logic, which trips the recirculation pumps at power levels greater than 40%.

(5) The reactor will scram unless the unit load is less than some preselected value (typically 40%), below which the control valve fast closure pressure transient does not threaten the fuel thermal limits.

(6) The trip setting of the APRM channels will be automatically reduced as recirculation flow decreases (flow referenced scram). Power level will have been reduced by a reactor scram and RPT initiation.

The trip settings discussed in Subsection 7.2.1 are not changed to accommodate abnormal operating conditions. Actions required during abnormal conditions are discussed in plant abnormal operating procedures. Transients requiring activation of the RPS are discussed in Chapter 15. The discussions there designate which system and instrumentation are required to mitigate the consequences of these transients.

#### 7.2.2.1.2 Other Considerations

Operability of the anticipatory signals from the turbine control valve fast closure or turbine stop valve closure following a safe shutdown earthquake is not a system design basis. As discussed in Subsection 5.2.2.2.2.2, closure of all the MSIV without MSIV position sensor trip produces a similar effect which is slightly more severe. The design basis analysis is conducted for the MSIV closure.

### 7.2.2.2 Conformance to Regulatory Codes, Guides, and Standards

#### 7.2.2.2.1 Regulatory Guides

(1) Regulatory Guide 1.22—Periodic Testing of Protection System Actuation Functions*

The system is designed so that it may be tested during plant operation from sensor device to final actuator device. The test must be performed in overlapping portions so that an actual reactor scram will not occur as a result of the testing.

(2) Regulatory Guide 1.47—Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems†

Automatic indication is provided in the control room to inform the operator that the system is out of service. Indicator lights indicate which part of a system is not operable.

Regulatory Position C.4

All the annunciators can be tested by depressing the annunciator test switches in the control room.

The following discussion expands the explanation of conformance to Regulatory Guide 1.47 to reflect the importance of providing accurate information for the operator and reducing the possibility for the indicator equipment to adversely affect its monitored safety system.

(a) Individual indicator lights are arranged together on the principal control console to indicate which function of the system is out of service, bypassed, or otherwise inoperable. The automatic indicators remain lit and cannot be cleared until the function is operable. All bypass and

* Includes conformance with BTP ICSB 22.

† Includes conformance with BTP ICSB 21.

inoperability indicators, both at a system level and component level, are grouped only with items that will prevent a system from operating if needed.

(b) A manual switch is provided for manual actuation to cover out-of-service conditions which could not be automatically annunciated.

(c) These indication provisions serve to supplement administrative controls and aids the operator in assessing the availability of component and system level protective actions. This indication does not perform a safety function.

(d) All system out-of-service annunciator circuits are electrically independent of the plant safety systems to prevent the possibility of adverse effects.

(e) Each indicator is provided with dual lamps. Testing will be included on a periodic basis, when equipment associated with the indication is tested.

(3) Regulatory Guide 1.53—Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems.

Compliance with NRC Regulatory Guide 1.53 is met by specifying, designing, and constructing the Reactor Protection System to meet the single-failure criterion described in Section 4.2 of IEEE-279 (Criteria for Protection Systems for Nuclear Power Generating Stations) and IEEE-379 (Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Class 1E Systems). Redundant sensors are used and the logic is arranged to ensure that a failure in a sensing element or the decision logic or an actuator will not prevent protective action. Separated channels are employed so that a fault affecting one channel will not prevent the other channels from operating properly. A complete discussion of the RPS power supplies is presented in Subsection 7.2.1.1.

(4) Regulatory Guide 1.62—Manual Initiation of Protective Actions.

Means are provided for manual initiation of reactor scram through the use of two armed pushbutton switches and the reactor mode switch. Operation of both pushbutton switches or placing the mode switch in the “SHUTDOWN” position accomplishes the reactor scram. These switches are located on the principal control room console.

The amount of equipment common to initiation of both manual scram and automatic scram is limited to actuated load power sources, actuated loads and cabling between the two. There is no shared trip or scram logic equipment for manual scram and automatic scram. No single failure in the manual,

automatic, or common portions of the protection system will prevent initiation of reactor scram by manual or automatic means.

Manual initiation of reactor scram, once initiated, goes to completion as required by IEEE-279, Section 4.16.

(5) Regulatory Guide 1.75—Physical Independence of Electric Systems

The RPS complies with the criteria set forth in IEEE-279, Paragraph 4.6, and Regulatory Guide 1.75, which endorses IEEE-384. Class 1E circuits and Class 1E-associated circuits are identified and separated from redundant and non-Class 1E circuits. Isolation devices are provided in the design where an interface exists between redundant Class 1E divisions and between non-Class 1E and Class 1E or Class 1E-associated circuits. Independence and separation of safety-related systems is discussed in Subections 8.3.1.3 and 8.3.1.4.

Physical and electrical independence of the instrumentation devices of the system is provided by channel independence for sensors exposed to each process variable. Separate and independent raceways are routed from each device to the respective remote multiplexing units (RMUs). Each channel has a separate and independent control room panel. Trip logic outputs are separated in the same manner as are the channels. Signals between redundant RPS divisions are electrically and physically isolated by Class 1E isolators or by fiber optic cables.

(6) [*Regulatory Guide 1.105*]*—Refer to Subsection 7.1.2.10.9 for assessment of Regulatory Guide 1.105.

(7) Regulatory Guide 1.118—Refer to Subsection 7.1.2.10.10 for assessment of Regulatory Guide 1.118.

Regulatory Position C.5 for APRM

With respect to conformance to Position C.5, the inherent time response of the incore sensors used for APRM (fission detectors operating in the ionization chamber mode) is many orders of magnitude faster than the APRM channel response time requirements and the signal conditioning electronics. The sensors cannot be tested without disconnecting and reconnecting to special equipment.

* See Subsection 7.1.2.10.9.

#### 7.2.2.2.2 Conformance to 10CFR50 Appendix A, General Design Criteria

(1) Criterion 2—Protection against Natural Phenomena

Wind and tornado loadings are discussed in Section 3.11, flood design in Section 3.4, and seismic qualification of instrumentation and electrical equipment in Section 3.10.

(2) Criterion 4—Environmental and Missile Design Bases

The RPS is designed to assure that the effects of natural phenomena and of normal operation, maintenance, testing and postulated accident conditions on redundant channels, divisions and equipment of the RPS will not result in the loss of the safety function of the system.

The redundant divisions of the RPS are electrically and physically separated from each other such that (1) no design basis event is capable of damaging equipment in more than one division and (2) no single failure, test, calibration or maintenance operation can prevent the safety function of more than one division.

(3) Criterion 13—Instrumentation and Control

Instrumentation is provided to monitor variables and systems over their respective anticipated ranges for normal operational, anticipated operational occurrences, and accident conditions to assure adequate safety. Each system input is monitored and annunciated.

(4) Criterion 15—Reactor Coolant System Design

The system acts to provide sufficient margin to assure that the design conditions of the RCPB are not exceeded during any condition of normal operation, including anticipated operational occurrences. If the monitored variables exceed their predetermined settings, the system automatically responds to maintain the variables and systems within allowable design limits.

(5) Criterion 19—Control Room

The control room is designed in accordance with this criterion. The design basis is provided in Section 1.2. If necessary, a reactor scram can be initiated from outside the control room by opening the circuit breakers in the A and B scram solenoid power distribution circuits. After scram initiation, capability for hot shutdown and subsequent cold shutdown from remote locations is provided by the Remote Shutdown System (Subsection 7.4.1.4). These functions are not within the scope of the RPS.

(6) Criterion 20—Protection System Functions

The system constantly monitors the appropriate plant variables to maintain the fuel barrier and primary coolant pressure boundary and initiates a scram automatically when the variables exceed the established setpoints.

(7) Criterion 21—Protection System Reliability and Testability

The system is designed with four redundant instrument channels and four independent and separated output channels. No single failure can prevent a scram. Individual components and select groups of components can be tested during plant operation to assure equipment and system reliability.

(8) Criterion 22—Protection System Independence

The redundant portions of the system are separated so that no single failure or credible natural disaster can prevent a scram except the turbine scram inputs which originate from the non-seismic Turbine Building. Reactor pressure and power are diverse to the turbine scram variables. In addition, drywell pressure and water level are diverse variables.

(9) Criterion 23—Protection System Failure Modes

The system is fail-safe on loss of power, in that loss of electrical power or air supply will not prevent a scram. Postulated adverse environments will not prevent a scram.

(10) Criterion 24—Separation of Protection and Control Systems

The system has no control function. It has interlocks with control systems through isolation devices. For each interlock with a control system, separate signals are provided by redundant portions of the RPS.

(11) Criterion 25—Protection Control System Redundancy and Capability

The RPS conforms to the requirements of GDC 25. The method of conformance is as follows:

The redundant portions of the system are designed such that no single failure can prevent a scram. Functional diversity is employed by measuring flux, pressure, and level in the reactor vessel, which are all reactivity-dependent variables.

The RPS provides protection against the onset and consequences of conditions that threaten the integrity of the fuel barrier and the reactor

coolant pressure boundary. Any monitored variable which exceeds the scram setpoint will initiate an automatic scram and not impair the remaining variables from being monitored (i.e., if one channel fails, the remaining portions of the RPS will function).

(12) Criterion 29—Protection Against Anticipated Operational Occurrences

The system will initiate a reactor scram in the event of anticipated operational occurrences.

#### 7.2.2.2.3 Conformance to Industry Codes and Standards

##### 7.2.2.2.3.1 IEEE-279, Protection Systems for Nuclear Power Generating Stations

The Reactor Protection (trip) System conforms to the requirements of this standard. The following is a detailed discussion of this conformance.

(1) General Functional Requirement (Paragraph 4.1)

The entire RPS, including its logic, trip actuator logic, and trip actuators, is designed to comply with this requirement through automatic removal of electric power to the CRD scram pilot valve solenoids when a sufficient number of RPS variables exceeds the specified trip setpoint.

(2) Single—Failure Criterion (Paragraph 4.2)

The RPS has four completely separate divisions with separate sensors whose only interaction is at the trip logic level via optical isolation. The system is in full compliance with the single-failure criterion and Regulatory Guide 1.53 (Subsection 7.2.2.2.1(3)).

(3) Quality of Components and Modules (Paragraph 4.3)

All RPS components and modules and such safety-related equipment of other systems providing inputs to the RPS are designed to maintain necessary functional capability under the extremes of conditions (as applicable), relating to environment energy supply, malfunctions, and accidents, within which the equipment has been designed and qualified to operate continuously and without degradation.

(4) Equipment Qualification (Paragraph 4.4)

Instrument sensors and electrical components of the RPS and interfacing systems which are used for RPS functions are qualified for nuclear safety-related service (important to safety) for the function times and for the environmental zones in which they are located. The RPS electrical Class 1E

equipment is qualified by type test data, previous operating experience or analysis, or any combination of these three methods to substantiate that all equipment which must operate to provide the safety system actions will be capable of meeting, on a continuing basis, the necessary performance requirements.

(5) Channel Integrity (Paragraph 4.5)

All RPS instrument channels, components and equipment and such safety-related equipment of other systems providing inputs to the RPS are designed to maintain necessary functional capability under the extremes of conditions (as applicable), relating to environment energy supply, malfunctions, and accidents, within which the equipment has been designed and qualified to operate continuously and without degradation.

(6) Channel Independence (Paragraph 4.6)

The RPS is designed to assure that the effects of natural phenomena and of normal operation, maintenance, testing and postulated accident conditions on redundant channels, divisions and equipment of the RPS will not result in the loss of the safety function of the system.

The redundant divisions of the RPS are electrically and physically separated from each other such that (1) no design basis event is capable of damaging equipment in more than one division and (2) no single failure, test, calibration or maintenance operation can prevent the safety function of more than one division.

Instrument channels that provide signals for the same protective function are independent and physically separated to accomplish the decoupling of the effects of unsafe environmental factors, electric transients and physical accident consequences and to reduce the likelihood of interactions between channels during maintenance operations or in the event of channel malfunctions.

(7) Control and Protection System Interaction (Paragraph 4.7)

The channels for the RPS trip variables are electrically isolated and physically separated from the plant control systems in compliance with this design requirement.

Multiple redundant sensors and channels assure that no single failure can prevent protective action.

Multiple failures resulting from a single credible event could cause a control system action (closure of the turbine stop or control valves) resulting in a condition requiring protective action and concurrent prevention of operation of a portion of the RPS (scram signal from the turbine stop or control valves) [Subsection 7.2.1.1.4.2(6)]. The reactor vessel high-pressure and high-power trips provide diverse protection for this event.

(8) Derivation of System Inputs (Paragraph 4.8)

The following RPS trip variables are direct measures of a reactor overpressure condition, a reactor overpower condition, a gross fuel damage condition, or abnormal conditions within the reactor coolant pressure boundary:

(a) Reactor vessel low water level trip

(b) Main steamline high radiation trip

(c) Neutron monitoring (APRM) system trip

(i) Neutron flux trip
(ii) Simulated thermal power

(d) Neutron Monitoring (SRNM) System trip

(i) Neutron flux trip
(ii) Short neutron flux period
(iii) Channel inoperative

(e) Drywell high pressure trip

(f) Reactor vessel high pressure trip

Other variables that could affect the RPS scram function itself, are thus monitored to induce scram directly include:

(g) Low charging pressure to rod HCU accumulators

(h) High suppression pool temperature

The detection of MSIV position and turbine stop valve position is an appropriate variable for the Reactor Protection System. The desired variable is loss of the reactor heat sink; however, isolation or stop valve closure is the logical variable to inform that the steam path has been blocked between the reactor and the heat sink.

Due to the normal throttling action of the turbine control valves with changes in the plant power level, measurement of control valve position is not an appropriate variable from which to infer the desired variable, which is rapid

loss of the reactor heat sink. Consequently, a measurement related to control valve closure rate is necessary.

Protection system design practice has discouraged use of rate-sensing devices for protective purposes. In this instance, it was determined that detection of hydraulic actuator operation would be a more positive means of determining fast closure of the control valves.

Loss of hydraulic pressure in the electrohydraulic control (EHC) oil lines, which initiates fast closure of the control valves, is monitored. These measurements provide indication that fast closure of the control valves is imminent.

This measurement is adequate and is a proper variable for the protective function, taking into consideration the reliability of the chosen sensors relative to other available sensors and the difficulty in making direct measurements of control valve fast-closure rate.

The turbine stop valve closure trip bypass and control valve fast closure trip operating bypass permit continued reactor operation at low-power levels when the turbine stop or control valves are closed. The selection of turbine first-stage pressure is an appropriate variable for permissive of this bypass function. In the power range of reactor operation, turbine first-stage pressure is essentially linear with increasing reactor power. Consequently, this variable provides the desired measurement of power level (i.e., whenever turbine first-stage pressure is below a specified value, the valve closure trip signals are automatically bypassed).

(9) Capability for Sensor Checks (Paragraph 4.9)

The RPS fully meets this requirement in that it conforms with Regulatory Guides 1.118 and 1.22. The four-channel logic allows cross-checking between channels and the ability to take any one channel out of service. When a channel is taken out of service, this fact is annunciated and the two-out-of-four logic reverts to two-out-of-three.

(10) Capability for Test and Calibration (Paragraph 4.10)

The RPS fully meets this requirement in that it conforms with Regulatory Guides 1.22 and 1.118. Capability for test and calibration is similar to that of sensor checks in that the four-channel logic allows cross-checking between channels and the ability to take any one channel out of service during reactor operation. Such a condition is annunciated and automatically causes the channel trip logic to revert from two-out-of-four to two-out-of-three.

Most sensors have a provision for actual testing and calibration during reactor operation. The exceptions are defined as follows:

(a) During plant operation, the operator can confirm that the MSIV and turbine stop valve limit switches operate during valve motion. Precise calibration of these sensors requires reactor shutdown.

(b) Testing of the main steamline high-radiation monitors can be performed during full power operation by cross-comparison of sensors. Calibration of the electronics portion of each channel can be performed during reactor operation by switching in a current source in place of the normal signal from the sensor. Calibration of the sensor itself can be performed during shutdown.

(c) Independent functional testing of the air header dump valves can be performed during each refueling outage. In addition, operation of at least one valve can be confirmed following each scram occurrence. These requirements are discussed in Chapter 16.

(11) Channel Bypass or Removal from Operation (Paragraph 4.11)

The two-out-of-four logic of the RPS is designed such that an entire division or its channel trip signals (except the NMS related trip functions and the manual reactor trip functions) can be bypassed to prevent initiation of protective action as a result of maintenance, testing or calibration operations.

A sensor channel bypass may be accomplished by separate switches provided for each divisional channel of the RPS.

Placing a channel sensors bypass switch in its BYPASS position manually reduces the normal coincident channel to division combination logic for reactor trip from two-out-of-four (2/4) to two-out-of-three (2/3) in all four divisions. The coincident channel-to-division combination trip logic cannot be reduced further than 2/3, as only one sensor channel is capable of being bypassed at any one time. The bypass condition is automatically annunciated for the individual channel being bypassed.

A division trip logic bypass may be accomplished by separate switches provided for each division of RPS logic. Placing a trip logic bypass switch in BYPASS manually reduces the normal scram logic to a coincidence of two-out-of-three tripped divisions. The coincident scram logic cannot be reduced further than two-out-of-three, as only one division is capable of being bypassed at any one time. The bypass condition is automatically annunciated for the individual division being bypassed.

Transmitters are normally tested during reactor operation by cross-comparison of channels. However, transmitters, level switches, and pressure switches may be valved out of service and returned to service under administrative control procedures. Since only one sensor is valved out of service at any given time during the test interval, protective capability for the RPS trip variables is maintained through the remaining redundant instrument channels.

(12) Operating Bypasses (Paragraph 4.12)

The following RPS trip variables have no provision for an operating bypass:

(a) Reactor vessel low water level trip

(b) Main steamline high radiation trip

(c) Neutron monitoring (APRM system trip)

(d) Not Used

(e) Drywell high-pressure trip

(f) Reactor vessel high-pressure trip

(g) High suppression pool temperature

An operating bypass of the low RCS accumulator charging pressure trip is provided in the control room for the operator to bypass the trip outputs during SHUTDOWN and REFUEL modes of operation. Control of this bypass is achieved with bypass switches through administrative means. Its only purpose is to permit reset of the RPS following reactor scram because the low charging water pressure condition would persist until the scram valves are reclosed. The bypass is manually initiated and must be manually removed (via switches or placing the mode switch in STARTUP) to commence withdrawal of control rods after a reactor shutdown.

An operating bypass is provided for the MSIV closure trip. The bypass requires that the reactor mode switch, which is under the administrative control of the operator, be placed in the SHUTDOWN, REFUEL, or STARTUP positions. The only purpose of this bypass is to permit the RPS to be placed in its normal energized state for operation at low-power levels with the MSIVs closed or not fully open.

An operating bypass is provided for the SRNM trip when the reactor mode switch is placed in the RUN position.

For each of these operating bypasses, separate signals are provided from the mode switch to each division of RPS logic to assure that all of the protection system criteria are satisfied.

An operating bypass of the turbine stop valve and control valve fast closure trip is provided whenever the turbine is operating at a low initial power level (i.e., with the mode switch in SHUTDOWN, REFUEL, or STARTUP positions). The purpose of the bypass is to permit the RPS to be placed in its normal energized state for operation at low-power levels with the turbine stop valves not fully open.

Special provision has been made to effect bypass of any one of the four MSIV closure RPS trip channels. This permits flexibility for testing and allows continued reduced power operation in the event of possible malfunction of the MSIVs such that up to two of the four steamlines can be closed off, for test purposes or otherwise, without resulting in a full reactor scram condition, provided the load has been reduced to limit reactor pressure and steam flow. The remaining three main steamlines automatically revert to two-out of-three logic such that closure of a second MSIV will result in a “half-scram” condition. This special bypass of any one channel will be automatically removed if a sensor channel bypass (described in Subsection 7.2.2.2.3.1(11) is imposed on any other channel.

In general, whenever the applicable conditions for instrumentation scram bypasses are not met, the RPS shall automatically accomplish one of the following:

(a) Prevent the actuation of an operating bypass.

(b) Remove any active operating bypass.

(c) Obtain or retain the permissive conditions for the operating bypass.

(d) Initiate the protective function.

(13) Indication of Bypasses (Paragraph 4.13)

The mode switches produced by operating bypasses need not be annunciated because they are removed by normal reactor operating sequence.

Although operating bypasses do not require annunciation, certain operating bypasses are annunciated in the main control room. The CRD accumulator low charging water pressure trip operating bypass, the MSIV closure trip operating bypass, the turbine stop and control valve fast closure trips operating bypass, and the division of sensors bypass are individually annunciated to the operator. Individual SRNM and APRM instrument

channel bypasses are indicated by lights for each division on the main control room panels.

(14) Access to Means for Bypassing (Paragraph 4.14)

All instrumentation valves associated with the individual RPS trip and bypass sensors are either locked open or locked closed, depending upon their normal state. The operator has administrative control of the sensor instruments and valves.

All manual bypasses (previously discussed) are controlled by keylock switches under administrative control of the operator. The mode switch itself is keylock operative, since its position affects the operating bypass logic.

(15) Multiple Setpoints (Paragraph 4.15)*

All RPS trip variables are fixed except for the following, which are individually addressed.

The trip setpoint of each SRNM channel is generally fixed. However, there is also the scram initiated by intermediate high neutron flux level corresponding to 5E + 5 counts per second. This is only activated in a noncoincidence scram mode by a switch in the RPS SSLC cabinet. The conditions under which such trip is to be activated are included in plant operating procedures.

In the RUN mode, the APRM System simulated thermal-power trip varies automatically with recirculation flow (Section 7.6).

In modes other than RUN, the APRM setdown function automatically selects a more restrictive scram trip setpoint at a fixed 15%. The devices used to prevent improper use of the less restrictive setpoints are designed in accordance with criteria regarding performance and reliability of protection system equipment.

Operation of the mode switch from one position to another bypasses various RPS trips and channels and automatically alters NMS trip setpoints in accordance with the reactor conditions implied by the given position of the mode switch. All equipment associated with these setpoint changes are considered part of the protection system and are qualified Class 1E components.

(16) Completion of Protective Action Once it is Initiated (Paragraph 4.16)

* Includes conformance with BTP ICSB 12.

It is only necessary that the process sensors remain in a tripped condition for a sufficient length of time to trip the digital trip modules and operate the seal-in circuitry, provided the two-out-of-four logic is satisfied. Once this action is accomplished, the trip actuator logic proceeds to initiate reactor scram regardless of the state of the process sensors that initiated the sequence of events. The same holds true for the manual scram pushbuttons.

(17) Manual Actuation (Paragraph 4.17)

Two manual scram pushbutton controls are provided on the principal control room console to permit manual initiation of reactor scram at the system level. Both switches must be depressed to initiate a scram. Backup to these manual controls is provided by the SHUTDOWN position of the reactor system mode switch. Failure of the manual scram portion of the RPS cannot prevent the automatic initiation of protective action, nor can failure of an automatic RPS function prevent the manual portions of the system from initiating the protective action.

No single failure in the manual or automatic portions of the system can prevent either a manual or automatic scram.

(18) Access to Setpoint Adjustments, Calibration, and Test Points (Paragraph 4.18)

The RPS design permits the administrative control of access to all setpoint adjustments, module calibration adjustments and testpoints. These administrative controls are supported by provisions within the safety system design, by provisions in the generating station design, or by a combination of both.

(19) Identification of Protective Actions (Paragraph 4.19)

When any one of the redundant sensor trip modules exceeds its setpoint value for the RPS trip variables, a main control room annunciator is initiated to identify the particular variable. In the case of NMS trips to the RPS, the specific variable or variables that exceed setpoint values are identified as a function of the NMS.

Identification of the particular trip channel exceeding its setpoint is accomplished as a typed record from the process computer system.

When any manual scram pushbutton is depressed, a main control room annunciation is initiated and a process computer system record is produced to identify the tripped RPS trip logic.

Identification of the mode switch in shutdown position scram trip is provided by the process computer system trip logic identification printout, the mode switch in shutdown position annunciator, and all division trips.

(20) Information Readout (Paragraph 4.20)

The data presented to the control room operator is consistent with human factors criteria and complies with this design requirement (Chapter 18). The safety system logic and control system, which incorporates the Reactor Protection System, is designed with self-test features which enhance the operator's awareness of the system itself. Each division and interdivisional function is tested sequentially and repetitively.

(21) System Repair (Paragraph 4.21)

Generally, all components can be replaced, repaired, and adjusted during operation. Exceptions are listed below.

During periodic testing of the sensor channels for the following trip variables, all defective components can be identified. Replacement and repair of failed sensors can only be accomplished during reactor shutdown.

(a) Neutron Monitoring System detectors

(b) Turbine control valve fast closure sensors

(c) MSIV closure sensors

(d) Turbine stop valve closure sensors

Provisions have been made to facilitate repair of NMS components during plant operation except for the detectors. Replacement of the detectors can be accomplished during shutdown.

(22) Identification of Protection Systems (Paragraph 4.22)

The RPS logic is housed, along with that of the essential core cooling systems and the leak detection and isolation systems, in the safety system logic and control (SSLC) cabinets. There are four distinct and separate cabinets in accordance with the four electrical divisions. Each division is uniquely identified by color code including cables and associated cables. The SSLC cabinets themselves are clearly marked with the words "Safety System Logic and Control". Each of the component systems controls is clearly identified on the cabinets in accordance with their system grouping and labeling. Control room panels are identified by tags on the panels which indicate the function

and identify the contained logic channels. Redundant racks are identified by the identification marker plates of instruments on the racks.

#### 7.2.2.2.3.2 Conformance to Other IEEE Standards

(1) IEEE-323—Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations

The general guide for qualifying Class 1E equipment is presented in Section 3.11. Records covering all essential components are maintained.

(2) IEEE-344—Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations

Seismic qualification of Class 1E equipment requirements are satisfied by all Class 1E RPS equipment as described in Section 3.10.

#### 7.2.2.2.4 Conformance to Branch Technical Positions

(1) BTP-ICSB-12: Protection System Trip Point Changes for Operation with Reactor Coolant Pumps Out of Service

The RPS design conforms with this position in that setpoint changes to more restrictive values are accomplished automatically in conjunction with the mode switch position [Subsection 7.2.2.2.3.1(15)].

(2) BTP-ICSB-21: Guidance for Application of Regulatory Guide 1.47

The RPS design conforms with this position, as discussed in Subsection 7.2.2.2.1(2).

(3) BTP-ICSB-22: Guidance for Application of Regulatory Guide 1.22.

The RPS design conforms with this position, as discussed in Subsection 7.2.2.2.1(1).

(4) BTP-ICSB-26: Requirements for Reactor Protection System Anticipatory Trips

All hardware used to provide trip signals to the RPS is designed in accordance with IEEE-279 and is considered safety-related. This includes the sensors for turbine stop valve closure and turbine control valve fast closure even though these are located in the non-seismic Turbine Building. Since reactor high pressure and power trips are diverse to the turbine scram variables, locating the sensors in the turbine enclosure does not compromise the ability of the RPS to provide protection action when required.

### 7.2.2.3 Additional Design Considerations Analyses (RPS)

(1) Spurious Rod Withdrawals

Spurious control rod withdrawal will not normally cause a scram but may cause control rod withdrawal block rod block, as discussed in Section 7.7, and is not part of the RPS. A scram will occur, however, if the spurious control rod withdrawal causes the average flux to exceed the trip setpoint, or causes SRNM short period.

(2) Loss of Plant Instrument Air System

Loss of plant instrument air will cause gradual opening of the scram valves on the hydraulic control units which will insert all control rods. Full insertion will result as air pressure is lost at the scram valves.

(3) Loss of Cooling Water to Vital Equipment

Loss of cooling water will not directly affect the RPS.

(4) Plant Load Rejection

Electrical grid disturbances could cause a significant loss of load, which would initiate a turbine generator overspeed trip and control valve fast closure, which may result in a reactor scram. The reactor scram occurs to anticipate an increase in reactor vessel pressure due to shutting off the path of steam flow to the turbine. Any additional increase in pressure will be prevented by the safety/relief valves, which will open to relieve reactor pressure and close as pressure is reduced. The Reactor Core Isolation Cooling (RCIC) or High Pressure Core Flooder (HPCF) Systems will automatically actuate and provide vessel makeup water if required.

The fuel temperature or pressure boundary thermal/hydraulic limits are not exceeded during this event (Chapter 15).

(5) Turbine Trip

Initiation of turbine trip by the turbine system closes the turbine stop valves initiating a reactor scram. The stop valve closure scram anticipates a reactor pressure or power scram due to turbine stop valves closure. Any additional increase in reactor vessel pressure will be prevented by the SRVs, which will open to relieve reactor vessel pressure and close as pressure is reduced. The RCIC and HPCF System will automatically actuate and provide vessel makeup water if low water level occurs.

Initiation of turbine trip by loss of condenser vacuum causes closure of turbine stop valves and main steam isolation valves, initiating a reactor scram.

The fuel temperature or pressure boundary thermal / hydraulic limits are not exceeded during these events (Chapter 15).

## Table 7.2-1 Reactor Protection System Instrumentation Specifications

| | | |
|---|---|---|
| Reactor vessel high pressure | 0–10.3 MPa G | Pressure-transmitter/trip module |
| Drywell high pressure | 0–0.036 MPaG | Pressure-transmitter/trip module |
| Reactor vessel low water Level 3 | 0–0.033 MPa G | Level-transmitter/trip module |
| Low charging pressure to rod HCU accumulators | 0–245.2 MPa G | Pressure transmitter/ trip module |
| Turbine stop valve closure | Fully open to fully closed | Position switch |
| Turbine control valve fast closure | 0–10.98 MPa G | Pressure-switch |
| Main steamline isolation valve closure | Fully open to fully closed | Position-switch |
| Neutron Monitoring System | APRM or SRNM Trip/No Trip | See Section 7.6 |
| Main steamline high radiation | 0.01-$10^4$mGy/h | Gamma detector |
| High suppression pool temperature | 4 to 110°C | Temperature-transmitter/trip module |
| Turbine first-stage pressure | | Pressure-transmitter/ trip module |

## Table 7.2-2 Channels Required for Functional Performance of RPS

This table shows the number of sensors required for the functional performance of the reactor protection system.

| Channel Description | # Sensors |
|---|---|
| Neutron Monitoring System (APRM) | 4 |
| Neutron Monitoring System (SRNM)* | 10 |
| Nuclear System high pressure | 4 |
| Drywell high pressure | 4 |
| Reactor vessel low level | 4 |
| Low charging pressure to rod hydraulic control unit accumulator | 4 |
| Main steamline isolation valve position | 8 |
| Turbine stop valve position | 4 |
| Turbine control valve fast closure† | 8 |
| Turbine first-stage pressure (bypass channel) | 4 |
| Main steamline radiation | 4 |
| High suppression pool temperature | 64 |

* In all modes except RUN.

† Four limit switches on FASV and four oil pressure switches.

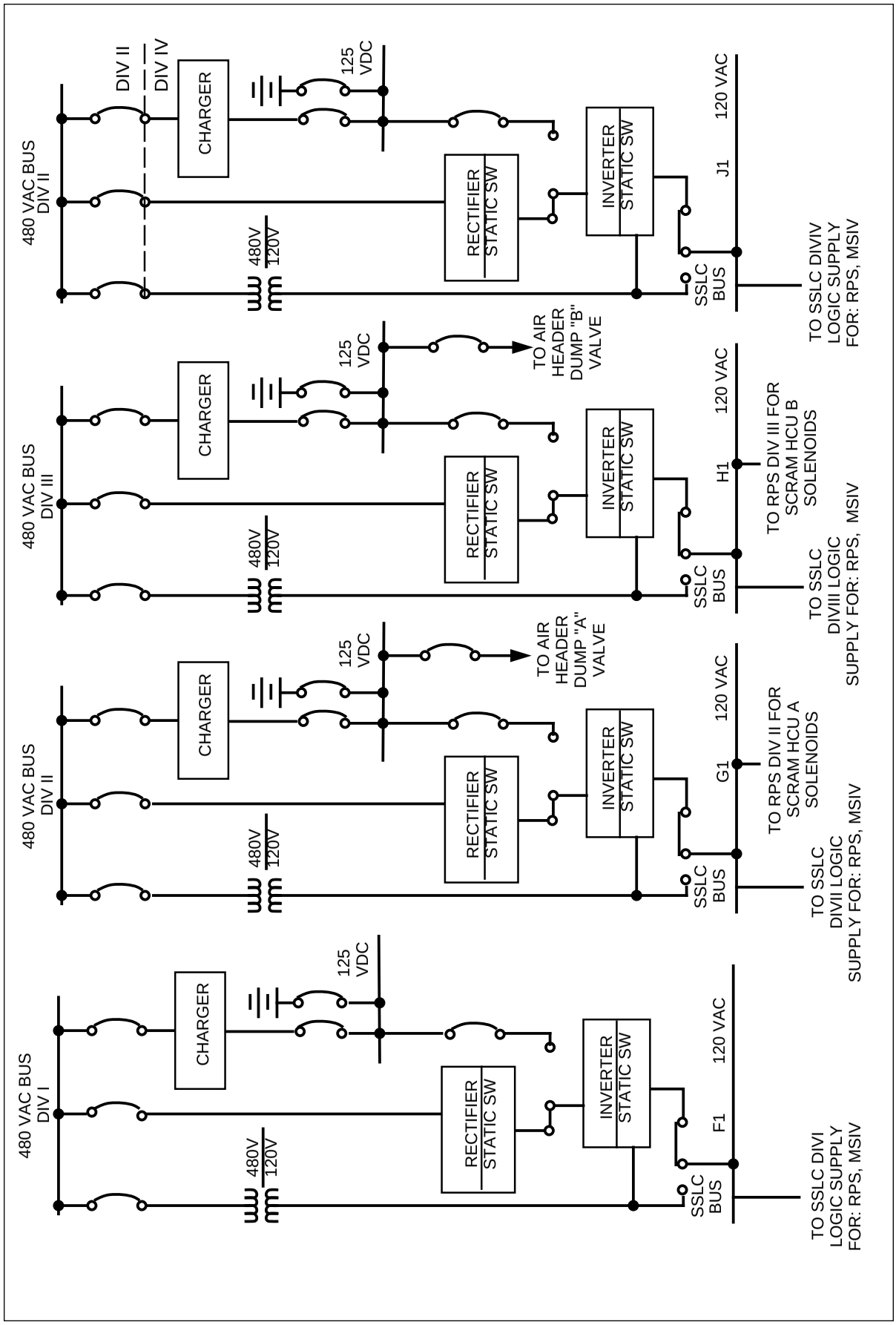



**Figure 7.2-1 ABWR SSLC Control Power Scheme (See also Figure 8.3-3)**

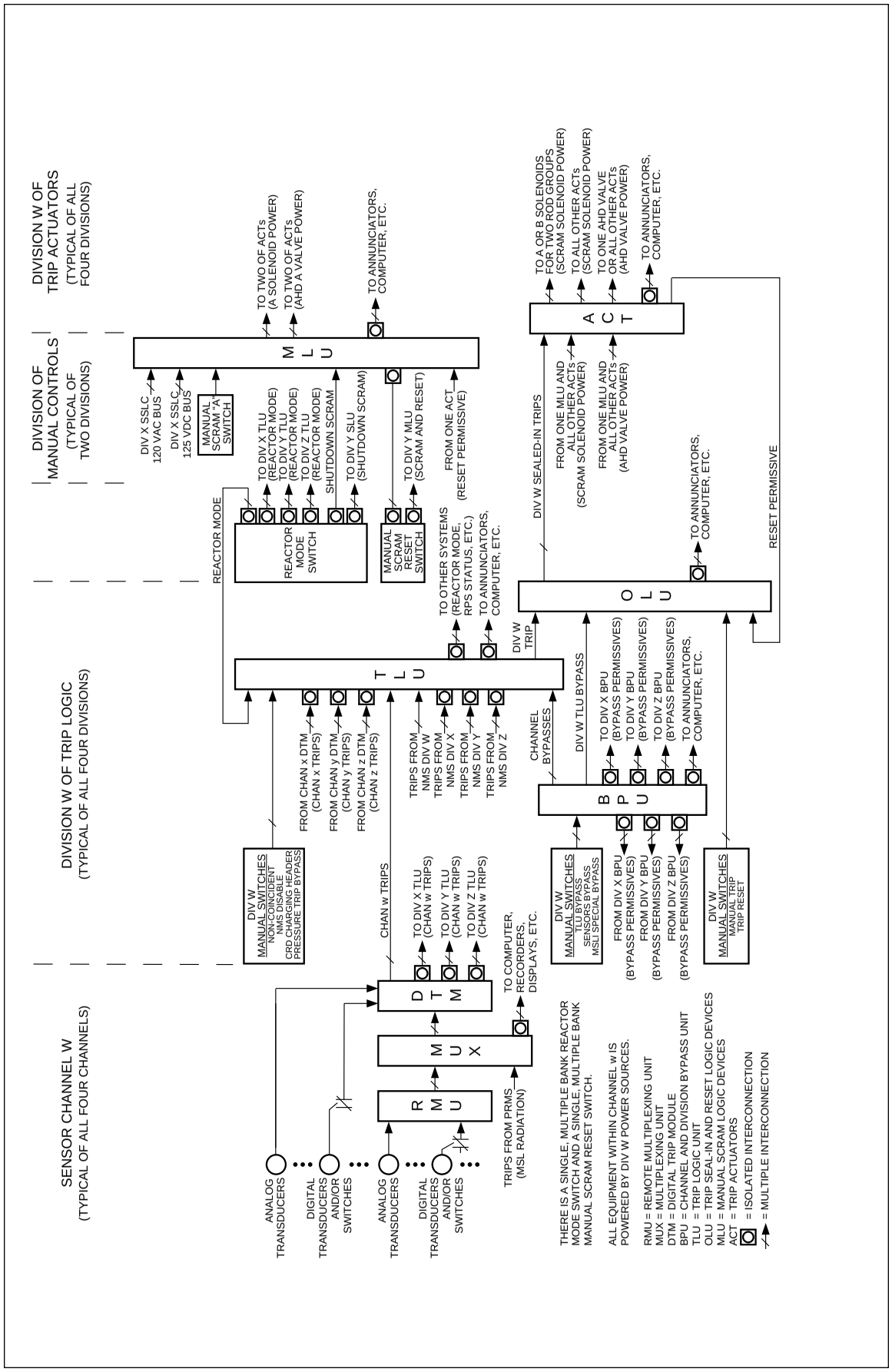



**Figure 7.2-2 Reactor Protection System Equipment Arrangement (From Sensors Through Trip Actuators)**

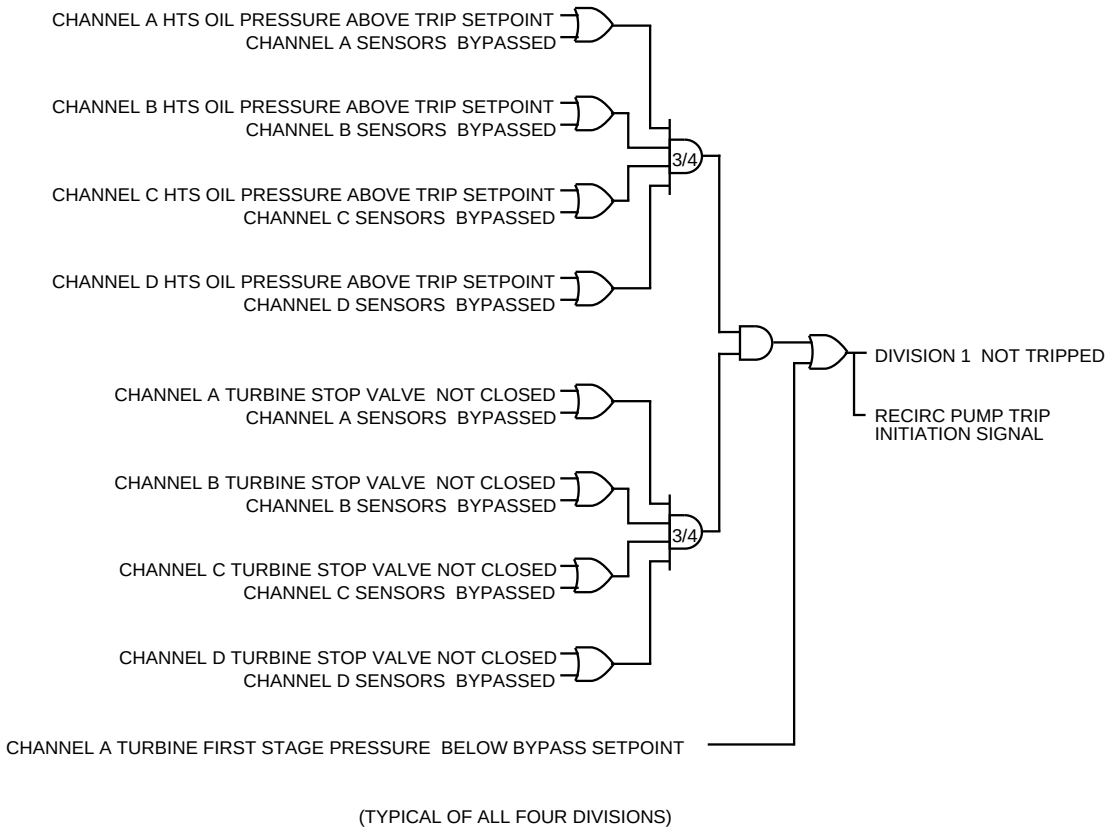



**Figure 7.2-3 Division 1 Trip Logic**
**Turbine Stop Valve Closure and Turbine Control Valve Fast Closure**

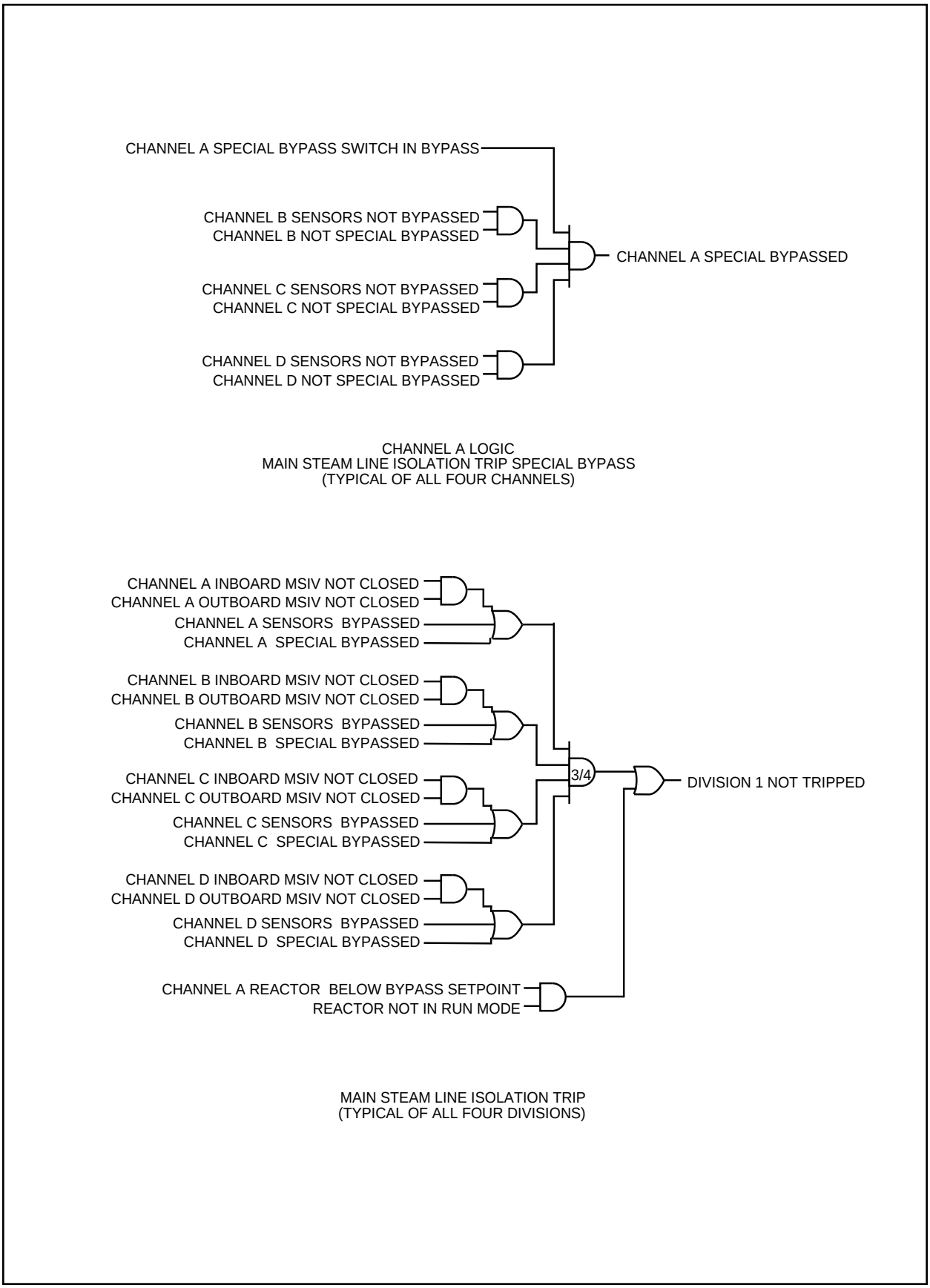



**Figure 7.2-4 Division 1 Trip Logic**

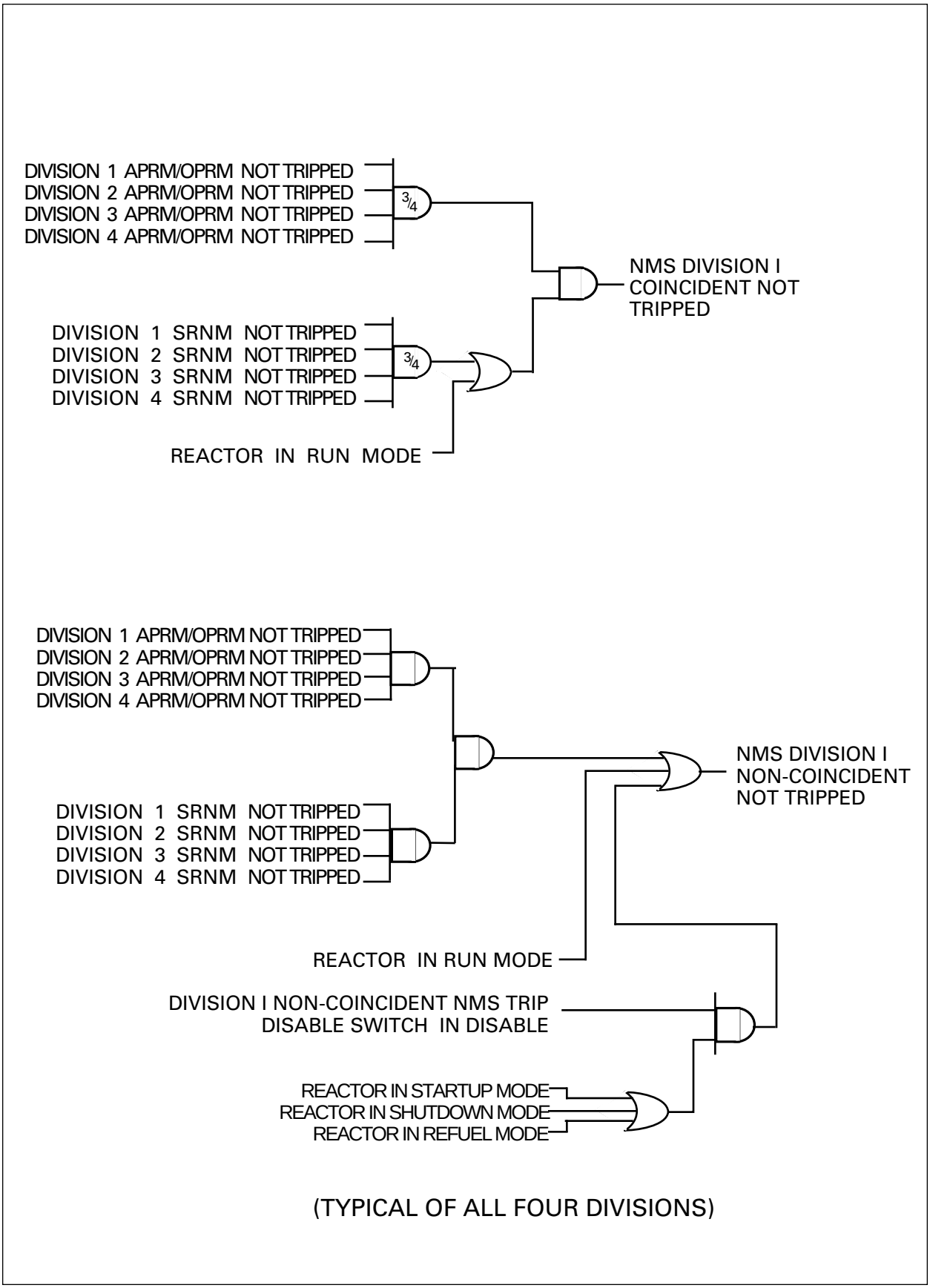
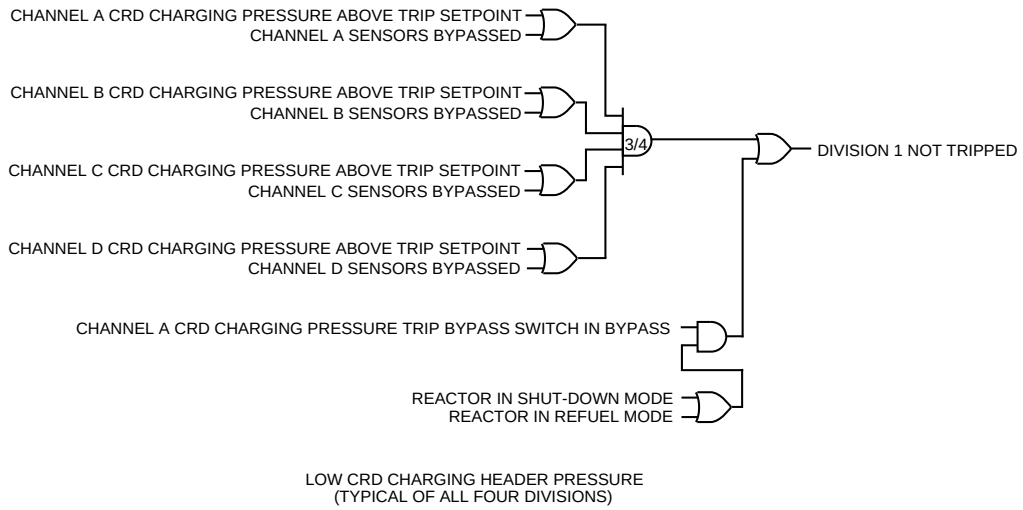
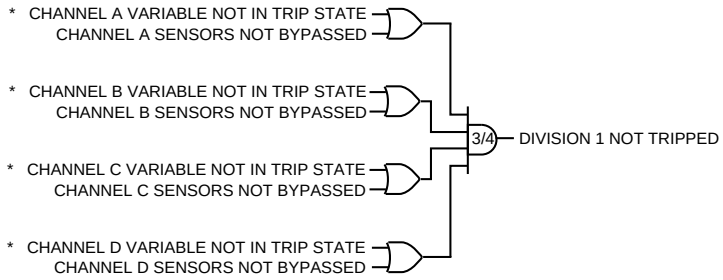



**Figure 7.2-5 Division 1 Trip Logic Coincident and Non-Coincident NMS Trips**




* TYPICAL OF – REACTOR PRESSURE ABOVE TRIP SETPOINT
– REACTOR WATER LEVEL BELOW TRIP SETPOINT
– DRYWELL PRESSURE ABOVE TRIP SETPOINT
– MAIN STEAM LINE RADIATION HIGH
– SUPPRESSION POOL TEMPERATURE HIGH

(TYPICAL OF ALL FOUR DIVISIONS)

**Figure 7.2-6 Division 1 Trip Logic**

**Figure 7.2-7 Not Used**

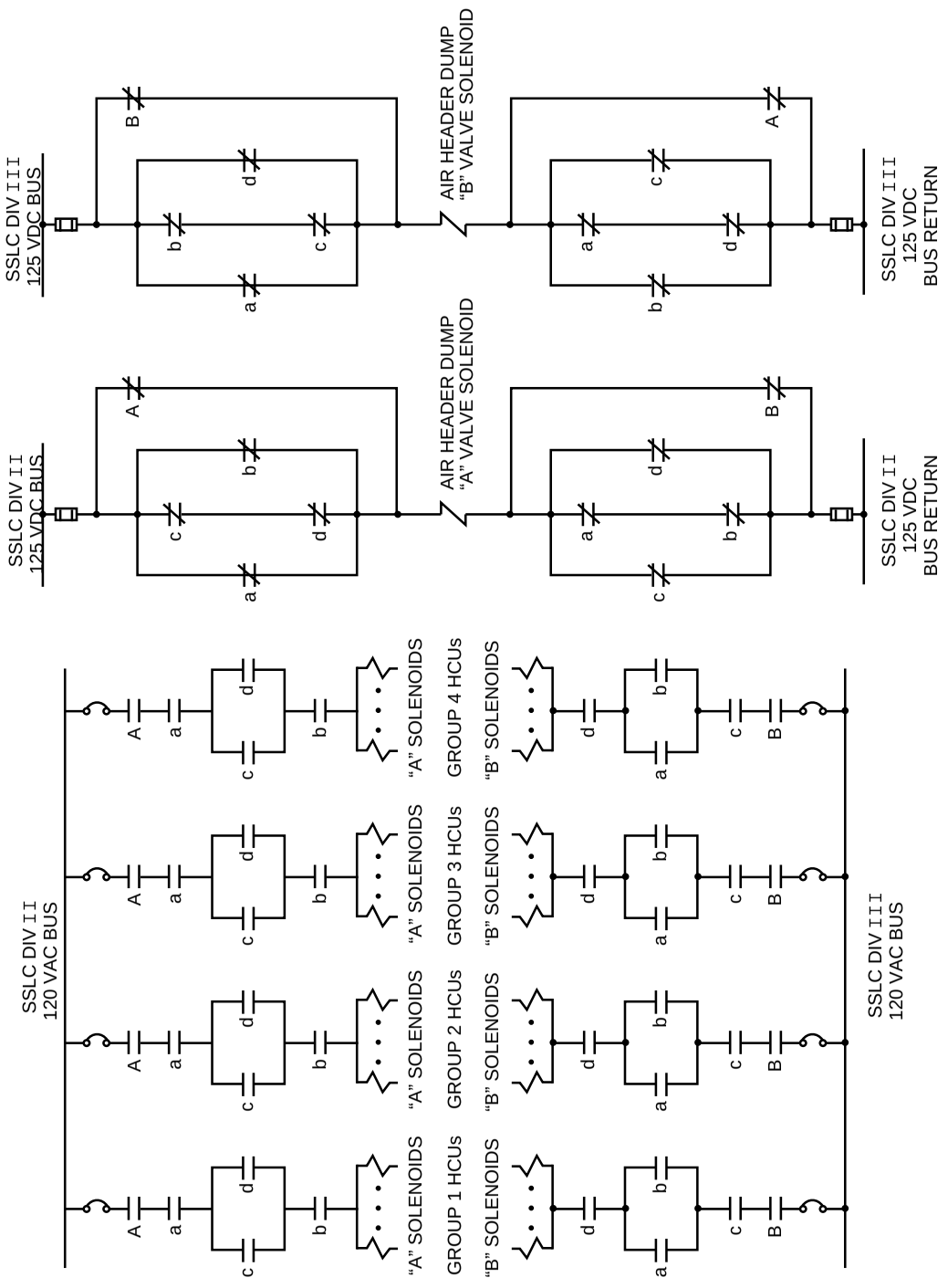



**Figure 7.2-8 SCRAM Solenoids and Air Header Dump Valves Power Distribution**

**The following figures are located in Chapter 21:**

**Figure 7.2-9 Reactor Protection System IED (Sheet 1–11)**

**Figure 7.2-10 Reactor Protection System IBD (Sheet 1–72)**

# 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 279 and provides reference to system diagrams which are included in the Safety Analysis Report.

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 SSLC Division 2 and 3, 120 VAC UPS buses (Section 8.3). The logic power is as described in Section 7.2 for the RPS portion of the SSLC.

(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 low 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 local multiplexer units which perform signal conditioning and analog-to-digital conversion. The formatted, digitized sensor input is multiplexed 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 within 36 seconds of receipt of initiation signal. 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 (they are normally in the open position unless the suppression pool suction valves are 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.

(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 36 seconds from receipt of the initiation signal.

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). 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 remote multiplexing units (RMUs). With a division-of-sensors bypass in place, calibrated, variable signals are injected in place of the sensor signals and monitored at the SSLC control room panels for linearity, accuracy, fault response, and downscale and upscale trip response.

Testing for functional operability of the control logic is accomplished by means of continuous automatic self-testing. The automatic system self-test discussed in Subsection 7.1.2.1.6 is also applicable for HPCF.

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, reactor water level sensing 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).

See Chapter 16 for 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 computer. 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) they will relieve pressure by actuation with electrical power 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 local multiplexer units which perform signal conditioning and analog-to-digital

conversion. The formatted, digitized sensor inputs are multiplexed 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 SSLC 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. Automatic initiation of ADS is inhibited unless there is a coincident low reactor water level signal and an average power range monitors (APRMs) ATWS permissive signal. 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 low-low water level (Level 1). 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 solenoid-operated pilot valves are energized to open a safety/relief valve. Linear variable differential transformers (LVDTs) mounted on the valve operators verify each valve position to the Performance Monitoring and Control System (PMCS), 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 low-low reactor water level). However, a keylocked 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. Automatic initiation of ADS is inhibited unless there is a coincident low reactor water level signal and an average power range monitors (APRMs) ATWS permissive signal. 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 rotating collar permissives and duality of button sets 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 low reactor vessel water level. 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 System.

(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. 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 SSLC. The logic is tested continuously by automatic self-test circuits. The STS (the sixth test), discussed in RPS testability (Subsection 7.1.2.1.6) is also applicable here for the ADS. The instrument channels are automatically verified every ten minutes. Testing of ADS does not interfere with automatic operation if required by an initiation signal. The pilot solenoid valves can be tested when the reactor is not pressurized.

(h) Environmental Considerations

The signal cables, solenoid valves, SRV operators and accumulators, and RV low-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 multiplex 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 a multipoint recorder and interfaces with the PMCS computer 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.

Refer to Chapter 16 for setpoints and margin.

(j) Parts of System Not Required for Safety

The non-safety-related portions of the ADS include the annunciators and the computer. 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 powered by the Division I 125 VDC system, except, for the isolation valves for steam supply. Inboard isolation valves are powered by 480 VAC Division I and outboard valves are powered by 125 VDC Division II.

(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 transducers used for the initiation and tripping and pressure transducers for isolation of the RCIC System are provided by the Nuclear Boiler System and are shared by other system channels within each division. They are located on instrument panels outside the drywell but inside the containment. 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 multiplexed optical data links described in Appendix 7A) to control circuitry in the main control room. Control system details are shown in Figure 7.3-3.

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 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 three exceptions:

(i) The flow controller in manual mode. This feature provides operator flexibility during system operation.

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

opening (an alarm sounds when either of these valves leaves the fully open position).

(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 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 transducers (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 transducer supplies a signal to a local multiplexer unit which performs signal conditioning and analog-to-digital conversion (Appendix 7A). The formatted, digitized sensor inputs are multiplexed 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 transducers 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 within 30 seconds. 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 as shown in Figure 7.3-3 (RCIC IBD). The turbine governor limits the turbine speed and adjusts the turbine steam control valve 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 across a flow element in the RCIC System pump discharge line.

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 actuated by the operator (provided auto-initiating signal is not present)

Turbine overspeed indicates a malfunction of the turbine control mechanism. High turbine exhaust pressure indicates a condition that threatens the physical integrity of 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. A turbine trip 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 detected by a standard turbine overspeed mechanical device. Four pressure sensors are used to detect high turbine exhaust pressure; any one sensor can initiate turbine shutdown. One pressure sensor is used to detect low RCIC System pump suction pressure.

High water level in the reactor vessel indicates that the RCIC System has performed satisfactorily in providing makeup water to the reactor vessel. Further increase in level could result in RCIC System turbine damage caused by gross carryover of moisture. The reactor vessel high water level setting which trips the turbine is near the top of the steam separators and is selected to prevent gross moisture carryover to the turbine. 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. See Chapter 6 (activated devices) for discussion of auto isolation logic.

(b) Logic and Sequencing

The scheme used for initiating the RCIC System is shown in Figure 7.3-3 (RCIC IBD).

(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 steam supply 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 and cooling excessively, a condensate drain pot, steamline drain, and appropriate valves are provided in a drain pipeline arrangement just upstream of the turbine supply valve. The controls position valves so that, during normal operation, steamline drainage is routed to the main condenser. The water level in the steamline drain condensate pot is controlled by a level switch and a direct acting solenoid valve which energizes to allow condensate to flow out of the drain pot. Upon receipt of an RCIC initiation signal and subsequent opening of the steam supply valve, the drainage path is shut off by redundant valves.

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

During test 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, the valves close as shown in Figure 7.3-3 (RCIC IBD). The pump suction from the condensate storage pool is automatically closed or interlocked closed if the suppression pool suction valve is fully open. 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. Four NBS sensors monitor each parameter and combine in two sets of two-out-of-four logic signals in the safety system logic and control (SSLC). A permissive signal from either set initiates the RCIC System. The sensor outputs themselves are shared by other systems in common with each division (see NBS P&ID Figure 5.1-3).

(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. The system is capable of initiation independent of AC power.

To assure that the RCIC System can be brought to design flow rate within 30 seconds 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 supply valve: 15 s
- RCIC pump discharge valves: 15 s
- RCIC pump minimum flow bypass valve: 15 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 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. The 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.

The instrumentation for isolation consists of the following:

– **Outboard RCIC turbine isolation valve:**

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

(ii) Main steamline pipe tunnel ambient temperature A or B high.

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

(iv) Two pressure transmitters and trip logic—RCIC turbine exhaust diaphragm (B and F) 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:**

Except for the suffix notations of A and E replacing B and F, a similar set of instrumentation causes the inboard valve to isolate.

Two pump suction valves are provided in the RCIC System. One valve lines up pump suction from the condensate storage pool, the other one from the suppression pool. The condensate storage pool is the preferred source. The control arrangement is shown in Figure 7.3-3 (RCIC IBD). Upon receipt of an RCIC initiation signal, the normally open condensate storage pool suction valve automatically opens if closed. Condensate storage pool 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 pool suction valve.

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

The auxiliary systems that support the RCIC System are the non-safety-related Gland Subsystem (which prevents turbine steam leakage) and the Lube Oil Cooling Water Subsystem. An RCIC initiation signal activates the vacuum pump of the barometric condenser and opens the cooling water supply valve, thereby initiating the gland seal and lube oil cooling functions. These systems remain on until manually turned off. However, the cooling water supply valve will close automatically on receiving a two-out-of-four high reactor water level signal.

(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 is monitored on the SSLC 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 tested every 10 minutes by automatic self-test circuits. The automatic self-test system (the sixth test) discussed in Subsection 7.1.2.1.6 is also applicable here for the RCIC System. With a division-of-sensors bypass in place, calibrated, variable ramp signals are injected in place of the sensor signals and monitored at the SSLC control room panels for linearity, accuracy, fault response, and downscale and upscale trip response.

(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. The RCIC System 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:

**Indication**

RCIC steamline supply pressure

RCIC valve (test bypass to suppression pool) position

RCIC pump discharge pressure

RCIC pump discharge flow

RCIC pump discharge minimum flow

RCIC turbine speed

RCIC turbine exhaust line pressure

RCIC turbine exhaust diaphragm pressure

**Indicating Lamps**

Position of all motor-operated valves

Position of all solenoid-operated valves

Turbine trip

Significant sealed-in circuits

Pump status

System status (power, test, isolation)

**Annunciators**

Annunciators are provided as shown in the RCIC system IBD (Figure 7.3-3) and the RCIC System P&ID (Figure 5.4-8).

(7) Setpoints

The reactor vessel low water level 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 (see Chapter 16 for actual setpoints and margin).

### 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 SSLC 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 (Level 1) is monitored by eight 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 multi-division transmitters are shared with other systems within the respective divisions. Four transmitters provide signals (one from each division) to RHR Divisions I and III. The other four transmitters provide similar signals to RHR Division II.

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 multiplexer units which perform signal conditioning and analog-to-digital conversion (Appendix 7A). The formatted, digitized sensor inputs are multiplexed 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 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 low water (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. Similarly, four water level sensors supply signals to RHR Divisions I and III. However, four different sensors supply the water level signals to RHR Division II. 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 low water level (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 10 second time delay, 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 low water level or drywell high pressure occurs, 10 seconds 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 36 seconds 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 valves from the suppression pool are normally open. To reposition the valves, a keylock switch must be turned in the control room. On receipt of an LPFL initiation signal, the reactor Shutdown Cooling System (SCS) valves and 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. Included in this set of valves are the valves that, if not closed, would permit the main system pumps to take suction from the reactor vessel itself (a lineup used during normal SCS operation).

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 channel trip setpoint is verified by automatic self-test functions in the SSLC which simulate programmed trip setpoints and monitor the response. The logic is also automatically tested by the self-test system 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. The operator may control the RHR pumps and injection valves manually after LPFL initiation to use RHR capabilities in other modes if the core is being cooled by other emergency core cooling systems.

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 computer. 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, also initiate closure of isolation valves to shut off leakage external to the containment.

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)

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

The power for the MSIVs pilot solenoid valve control logic is supplied from all four divisions of the SSLC 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 SSLC 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 3 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) Main Steamline Radiation

Main steamline (MSL) radiation is monitored by gamma sensitive radiation monitors in the Process Radiation Monitoring System (Section 7.6). The objective of the MSL Radiation Monitoring Subsystem is to monitor for the gross release of fission products from the fuel and, upon indication of such release, initiate appropriate action to limit fuel damage and further release of fission products.

The process radiation monitor detectors are physically located near the main steamlines just downstream of the outboard MSIVs. The detectors are geometrically arranged to detect significant increases in radiation level with any number of main steamlines in operation.

When a significant increase in the main steamline radiation level is detected, trip signals are transmitted to the Reactor Protection System (RPS) to indicate reactor trip and to the LDS to initiate closure of all MSIVs and the steamline drain valves.

(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

Large remote power-operated valves located in the drywell for the NBS, CUW, RCIC, and RHR Systems are fitted with drain lines from the valve stems. Each drain line is located between two sets of valve stem packing. Leakage through the inner packing is carried to the drywell equipment drain sump. Leakage during hydrotesting may be observed in drain line sight glasses installed in the drain line to the sump. A remote-operated solenoid valve on each line is provided to isolate a leaking line, and may be used during plant operation, in conjunction with the sump instrumentation, to identify the specific process leaking valve.

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 established at 95 L/min for equipment drain sumps and to 19 L/min for floor drain sumps. 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 Diaphragm Pressure Monitors

Pressure between the rupture disc diaphragms 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.

(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.

The ATIP System is provided with either low reactor water level or high drywell pressure 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) Four divisional radiation instrument channels monitor for high MSL radiation in the MSL tunnel area.

(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 diaphragm 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 computer. 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 multiplexer units 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 initiate the WDSC.

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

**Wetwell Spray B:** The initiation of wetwell spray is manual and does not have an interlock. 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

The operating sequence of wetwell and drywell spray following receipt of the LPFL initiating signals is as follows:

(i) The RHR pumps are operating.

(ii) Valves in other RHR modes are automatically repositioned to LPFL injection.

(iii) The service water emergency pumps are signaled to start.

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

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

(vi) Vessel injection takes place to flood the reactor

(vii) In the presence of high drywell pressure and/or high wetwell pressure, the injection valve is manually closed after the initial injection.

(viii) Drywell spray and wetwell spray valves are manually opened to perform the spray function.

The spray system will continue to operate until manually terminated by the operator or when a RHR initiation signal closes the wetwell spray valve or an injection valve not fully closed signal closes the drywell spray valves. The spray system will automatically terminate and realign to the injection mode, 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.

No interlock is provided for wetwell spray function.

(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 channel trip setpoint is verified by automatic self-test functions in the SSLC which simulate programmed trip setpoints and monitor the response. Testing for functional operability of the control logics is accomplished by the automatic self-test system (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).

See Chapter 16 for setpoints and margin.

(j) Parts of System Not Required for Safety

The non-safety-related portions of the WDCS-RHR include the annunciators and the computer. 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 manually 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 injection valves are manually closed and SP valves are opened.

(v) The SPC mode will continue to operate until the operator closes the SPC discharge valves or when reactor low water level reoccurs, in which case the injection valve will auto-open and the SP discharge valve will auto-close.

(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 by the automatic system self-test.

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 computer. 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 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 downstream 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 computer. 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 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 and CRD oil cooling, the non-safety-related loads are automatically isolated upon a LOCA. All non-safety-related loads 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 and II RCW flow signals to the MCR and Divisions I and II RCW flow signal to the RSS.

— RCW Hx 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. See Chapter 16 for setpoints and margin.

(k) Parts of System Not Required for Safety

The non-safety-related portions of the RCW System include the annunciators and the computer. 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 refrigerators 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 refrigerator units; each refrigerator unit includes the condenser, evaporator, centrifugal compressor, refrigerant pipings 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 refrigerator. Supply flow is controlled by the condensing pressure of the refrigerant. A flow switch provided at the chilled water line shuts down the refrigerator and chilled water pump 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 (refrigerator 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 refrigerator in the event of low flow in the chilled water line. A common trouble alarm for each refrigerator unit is annunciated in the control room upon detection of any refrigerator unit alarm or trip. A running signal from each RCW pump in each division is interlocked to trip the refrigerators if at least one RCW pump is not operating.

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

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

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

(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 refrigerator 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 two 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 Flammability Control System—Instrumentation and Controls

(See Subsection 6.2.5)

### 7.3.1.2 Design Basis Information

IEEE-279 defines the requirements for design bases. Using the IEEE 279 format, 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)] 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 margin between operational limits and the limiting conditions of operation for the ESF System instruments are listed 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 low water level and drywell high pressure are sensed, or when the 8 minute drywell high pressure bypass timer 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 8 minute drywell high pressure bypass timer and low 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-279):

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-279.

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 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 safety system logic and control (SSLC) 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 multiplexed and passed 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-279 and Regulatory Guide 1.75.

Other requirements of IEEE-279, 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 (which use pulse testing) 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 4.2 of IEEE-279 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 (e.g., the SRV solenoid pilot valves).

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. 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.*]*

* See Subsection 7.1.2.10.9.

(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) BPT 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.

(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 ADS valve pilot solenoids and the LPFL shutdown valves which cannot be opened while the reactor is pressurized. However, both can be tested during reactor shutdown. In addition, the ADS valve solenoids are monitored for continuity during the logic self-test.

(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-279)

The LDS is 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 safety system logic and control (SSLC) 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 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 multiplexed and 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-279 and Regulatory Guide 1.75. For further information see Subsection 9A.5.5.7.

Other requirements of IEEE-279 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-279)

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). This mode of the RHR System (unlike the LPFL mode which is automatically actuated by LOCA) is automatically actuated should high pressure conditions occur in the drywell and wetwell air space.

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-279 as described in Subsection 7.3.1.1.3.

A clarification should be made with regard to IEEE-279, Section 4.19. 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 WDSC 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-279)

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-279 as described in Subsection 7.3.1.1.4.

A clarification should be made with regard to IEEE-279, Section 4.19. 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-279)

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-279. 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-279)

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 vavlves in both systems 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-279)

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 to be automatically isolated. A LOCA signal will isolate all RCW non-safety-related loads except the instrument air and CRD oil 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-279. 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-279)

The essential HVAC Systems (HVAC) have two 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 corresponding with electrical Divisions I & II, respectively. Electrical separation is maintained between the redundant divisions.

The HVAC System is designed to meet all applicable requirements of IEEE-279. 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-279)

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-279. 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-279)

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 279. 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 [*NEDC-31336, Julie Leong, "General Electric Instrument Setpoint Methodology", October 1986.*]*

* See Subsection 7.1.2.10.9.

**The following figures are located in Chapter 21:**

**Figure 7.3-1 High Pressure Core Flooder IBD (Sheets 1–17)**

**Figure 7.3-2 Nuclear Boiler System IBD (Sheets 1–37)**

**Figure 7.3-3 Reactor Core Isolation Cooling System IBD (Sheets 1–17)**

**Figure 7.3-4 Residual Heat Removal System IBD (Sheets 1–20)**

**Figure 7.3-5 Leak Detection and Isolation System IBD (Sheet 1–77)**

**Figure 7.3-6 Standby Gas Treatment System IBD (Sheets 1–11)**

**Figure 7.3-7 Reactor Building Cooling Water System/Reactor Service Water System IBD (Sheets 1–19)**

**Figure 7.3-8 Not Used**

**Figure 7.3-9 HVAC Emergency Cooling Water IBD (Sheets 1–11)**

**Figure 7.3-10 High Pressure Nitrogen Gas IBD (Sheets 1–3)**

# 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 3 of IEEE-279.

### 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). Independent sensors (i.e., ECCS sensors) provide reactor trip signals, via the Recirculation Flow Control System (RFCS), both to ARI valves (part of the Control Rod Drive System) and to the Rod Control and Information System (RCIS). The ARI valves (separate from the scram valves), cause reactor shutdown by hydraulic scram of the control rods. The RCIS, acting upon the same ARI signals that are provided to ARI valves, causes reactor shutdown by electromechanical (i.e., through the usage of FMCRD motors) insertion of control rods.

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 6900 VAC 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. The fuel pool intertie is applied only to Loops B and C (see Figure 5.4-10 for RHR System P&ID).

(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 it 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 System 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 Subsections 7.3.1.1.3 and 7.3.1.1.4.

(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.

The logic is tested by automatic self-test. The sixth test, 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 Class 1E power system buses E and F 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 multiplexing system remote multiplexing units (RMUs) for transmission to the main control room. Similarly, control signals from the main control room are routed from the RMUs, through the remote shutdown transfer devices, and then to the interfacing system equipment. Actuation of the transfer devices interrupts the connection to the RMUs 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

(c) The following function has transfer and control switches located at the Division 2 remote shutdown control panel: one air-operated relief valve. (The valve is 125 volt DC solenoid pilot operated.)

(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) 6.9 kV feeder breaker: Unit auxiliary transformer A to M/C E

(ii) 6.9 kV feeder breaker: Reserve auxiliary transformer A to M/C E

(iii) 6.9 kV feeder breaker: Emergency diesel generator A to M/C E

(iv) 6.9 kV feeder breaker: Combustion turbine generator to M/C E

(v) 6.9 kV load breaker: M/C E 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) 6.9 kV feeder breaker: Unit auxiliary transformer B to M/C F

(ii) 6.9 kV feeder breaker: Reserve auxiliary transformer A to M/C F

(iii) 6.9 kV feeder breaker: Emergency diesel generator B to M/C F

(iv) 6.9 kV feeder breaker: Combustion turbine generator to M/C F

(v) 6.9 kV load breaker: M/C F to P/C F20

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

(c) A 6.9 kV M/C (E,F) voltmeter is provided on RSS panels A,B, respectively.

(8) Flammability Control System (FCS)

(a) The following FCS equipment function has transfer and control switches located on both remote shutdown panels as indicated:

(i) Valve (cooling water inlet) B

(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 alternate rod insertion (ARI) 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 scram system.

The RCIS and the active run-in function of the FMCRD motors 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-31906-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-279)

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-279, Section 4.7, signals which interface between ARI and RPS are optically isolated such that postulated failures within the ARI controls cannot affect the safety-related scram function.

The RCIS logic has been designed such that a single failure, only in the inverter controller part of a given rod logic, may result in insertion failure of that rod when the ARI function is activated. Also, two manual actions are required at the dedicated operator interface 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. However, the breaker coordination is assured through the use of zone selective interlocks (ZSI) (Subsection 8.3.1.1.1).

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

The ZSI feature assures that the FMCRDs power 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. The ZSI is a new technology which assures

breaker coordination, and thus meets the intent of position C-1 of Reg. Guide 1.75.

In addition, each FMCRD inverter has current limiting features to limit the FMCRD motor fault current. Continuous operation of all the FMCRD motors at the limiting fault current of the inverter shall not degrade operation of any Class 1E loads (i.e., the diesel generators shall be of appropriate design capacity).

### 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-279)

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-279 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 safety 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) RHR logic power failure.

(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) 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 or cooling water 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-279):

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.

A clarification should be made with regard to IEEE-279, Section 4.19. 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-279 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-279 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.

* See Subsection 7.1.2.10.9.

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 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-279)

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 |
| Flammability Control System | B, C | B |

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-279 and Regulatory Guide 1.75.

With regard to Paragraph 4.2 of IEEE-279, 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-279 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-279 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-31906-P-A, A. Chung, "Laguna Verde Unit 1 Reactor Internals Vibration Measurement", February 1991.

## 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*f* | 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)*f* | Closes (A) |
| Outboard suction isolation | Closes (A) | Closes (A) |
| Reactor injection | Closes (A) *f* | Closes (A) |

* Valves have manual control for opening.

† (A) denotes automatic.

‡ Valves have manual and auto control for opening.

*f* 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:**

**Figure 7.4-1 Standby Liquid Control System IBD (Sheets 1–6)**

**Figure 7.4-2 Remote Shutdown System IED**

**Figure 7.4-3 Remote Shutdown System IBD (Sheets 1–27)**

# 7.5 Information Systems Important to Safety

## 7.5.1 Systems Descriptions

Safety-related display systems are those systems which provide information for the safe operation of the plant during normal operation, anticipated operational occurrences, and accidents. The information systems important to safety include those systems which provide information for manual initiation and control of safety systems, to indicate that plant safety functions are being accomplished and to provide information from which appropriate actions can be taken to mitigate the consequences of anticipated operational occurrences and accidents. The Safety Parameter Display System (SPDS), information systems associated with the emergency response facilities and nuclear data link are information systems important to safety.

### 7.5.1.1 Post Accident Monitoring System

(1) Variable Types

Regulatory Guide 1.97 defines five “types” and three “categories” of plant variables for accident monitoring instrumentation. A discussion of these classifications is provided below. Each variable has been defined as to both type and classification. Plant variables are divided into types according to the purpose of the indication to the plant operator. Any one variable may belong to more than one type.

(a) Type A

Type A are those variables to be monitored that provide the primary information required to permit the control room operators to take the specified manual actions for which no automatic control is provided and that are required for safety systems to accomplish their safety functions for design basis accident events.

Primary information is information that is essential for the direct accomplishment of the specified safety function. It does not include those variables that are associated with contingency (or backup) action that may also be identified in written procedures or guidelines.

Type A variables are limited to those variables which are necessary (primary) to alert the control room operator of the need to perform preplanned manual actions for safety systems to perform their safety functions, such as, initiating suppression pool cooling and containment spray to permit the systems to perform safety functions for which no automatic system controls are provided. Variables that require actions specified by the Emergency Procedure Guidelines (EPGs) in response to

specific operating limits have also been considered in performing the assessment documented in this chapter.

Type A variables do not include variables (1) which may indicate whether a specific safety function is being accomplished (Type B), or (2) which may indicate the need for contingency or corrective actions, resulting from the failure of the plant (Type C) or system(s) (Type D) to respond correctly when needed, or (3) which may indicate to the operator that it is desirable to change or modify the operation / alignment of systems important to safety to maintain the plant in a safe condition after plant safety has been achieved. Subsection 7.5.2.1(1) discusses the selection of specific Type A variables for the ABWR.

(b) Type B

Type B are those variables that provide information to the control room operators to indicate whether plant safety functions are being accomplished, including reactivity control, core cooling, maintaining reactor coolant system integrity, and maintaining containment integrity.

(c) Type C

Type C are those variables that provide information to the control room operators to indicate that barriers to fission product release have the potential for being breached or have been breached. These barriers are the fuel cladding, primary coolant pressure boundary, and primary containment.

The sources of potential breach are limited to the energy sources within the cladding, coolant boundary, or containment.

(d) Type D

Type D are those variables that provide information to the control room operators to indicate the successful operation of individual safety systems or other systems important to safety.

Type D variables should provide information to permit the control room operators to ascertain the operating status of each individual safety system and other systems important to safety to that extent necessary to determine if each system is operating or can be placed in operation to help mitigate the consequences of an accident.

(e) Type E

Type E are those variables monitored to determine the magnitude of release of radioactive materials and to assess the continuation of such releases.These variables should permit the control room operators to monitor the effluent discharge paths and environs within the site boundary to ascertain if there have been significant releases (planned or unplanned) of radioactive materials and to continually assess such releases.

In particular, Type E variables monitor:

(i) The planned paths for effluent release

(ii) Plant areas inside buildings where access is required to service equipment necessary to mitigate the consequences of an accident

(iii) Onsite location where unplanned releases of radioactive materials are detected

(2) Categories of Variables

The design and qualification criteria for the instrumentation used to measure the various variables are divided into three categories that provide a graded approach to instrumentation criteria, depending on importance to safety of the variables.

In general, Category 1 provides for full qualification, redundancy, and continuous real-time display and requires onsite (standby) power. Category 2 provides for qualification but is less stringent in that it does not (of itself) include seismic qualification, redundancy, or continuous display and requires only a high-reliability power source (not necessarily standby power). Category 3 is the least stringent. It provides for high-quality commercial-grade equipment that requires only offsite power.

(a) Category 1 represents the most stringent criteria and is used for key variables. Key variables are those parameters that most directly indicate the accomplishment of a safety function. All Type A variables are considered to be Category 1. For Types B and C, the key variables are Category 1, while backup variables are generally Category 3.

(b) Category 2 provides less stringent criteria and generally applies to instrumentation designated for indication of system operating status. Most Type D variables are classified as Category 2.

(c) Category 3 provides criteria for high quality backup and diagnostic instrumentation or for other instrumentation where the state-of-the-art will not support requirements for higher qualified instrumentation.

(3) Design and Qualification Criteria

The detailed Design and Qualification Criteria for Category 1, 2 and 3 variables are provided in Reg. Guide 1.97 for:

(a) Equipment Qualification

(b) Redundancy

(c) Power Sources

(d) Channel Availability

(e) Quality Assurance

(f) Display and Recording

(g) Range

(h) Equipment Identification

(i) Interfaces

(j) Servicing, Testing, and Calibration

(k) Human Factors

(l) Direct Measurement

A detailed listing of the design and qualification criteria for Categories 1, 2 and 3 is provided in Table 7.5-1.

In addition to design and qualification criteria, Regulatory Guide 1.97 provides a comprehensive listing of “BWR variables” which address accident monitoring requirements. Table 7.5-2 was developed using Table 2 of Regulatory Guide 1.97 as a guide. Design and qualification criteria are addressed as category designations per the discussion above. Variables listed in Table 7.5-2 without comment meet the design and qualification requirements of Regulatory Guide 1.97. Any exceptions taken are noted in the comment column.

## 7.5.2 Systems Analysis

### 7.5.2.1 Post Accident Monitoring System

(1) Type A Variables

Type A variables are fundamentally plant parameters needed to alert the control room operators to take safety actions by manually initiating a system or function which otherwise would not be automatically initiated in the course of an event. The Regulatory Guide 1.97 does not specify Type A variables; rather, it requires that each plant develop its own list of Type A variables from a review of each plant design.

For this assessment, the list of Type A variables was identified from a review of accidents described in Chapter 15 and a review of the Emergency Procedure Guidelines (EPGs). The event descriptions of Chapter 15 and the Plant Nuclear Safety Operational Analysis (NSOA)of Appendix 15A were reviewed to determine the ABWR plant systems which would require manual initiation and the key variables associated with manual initiation of those systems. The Emergency Procedure Guidelines (EPGs) included in Chapter 18, Human Factors Evaluation, Appendix 18A, were also reviewed to identify any other variables requiring safety action. A summary of the Type A variables identified through this process are shown in Table 7.5-3. Details of the Type A variable assessment are provided in the following portion of this section.

(a) Type A Variable Evaluation and Analysis

Chapter 15 contains discussions of numerous events, not all of which are design basis accidents. Appendix 15A is a plant Nuclear Safety Operational Analysis (NSOA) which addresses these events in the following categories:

(i) Normal operations
(ii) Anticipated Operational Transients (Table 5.7-4)
(iii) Abnormal Operational Transients (Table 5.7-5)
(iv) Design Basis Accidents (Table 5.7-6)
(v) Special Events (Table 5.7-7)

Variables associated with normal operations are excluded from further investigation because those activities are planned actions which would not normally be expected to cause a threat to the general public.

Because probabilistic risk assessments show that the risk to the general public is dominated by transients rather than design basis accidents, all of the above categories (except normal operations) were considered to determine what parameters required operator action. Tables 7.5-4 through 7.5-7 list the events considered and the primary variables associated with called-for manual action. The manual action variables are taken from either the NSOA or the Chapter 15 event descriptions.

The required manual actions are summarized in Table 7.5-8 along with the associated variables.

The EPGs were also reviewed to determine if there are other variables not specifically identified by Chapter 15 which are associated with required operator actions. Table 7.5-8 includes these additional variables and actions which result from a review of the following guidelines included in Appendix 18A:

(i) RPV Control

(ii) Primary Containment Control

(iii) Radioactivity Release Control

(iv) Secondary Containment Control

Some of these variables, especially those related to emergency action, are considered beyond the scope of the regulatory guide by virtue of requiring "contingency actions that are identified in written procedures."

The final list of Type A variables was derived from the variables indicated on Table 7.5-8 and is summarized on Table 7.5-3.

For the ABWR, actions to isolate systems will be accomplished automatically by the LDS on high area temperatures ($T_{2C}$). Thus, this parameter is excluded from the Type A variable list. Other secondary containment area parameters ($R_{2C}$ $L_{2C}$) were deleted because they represent early actions which could be taken to reduce the amount of plant effluent release beyond those values used as a basis for the plant safety analysis. Thus, these parameters were considered to be contingency actions and not required to be Type A.

The offsite release rate ($R_E$) was also not included with the Type A Variable List because the emergency action (emergency depressurization) specified in the radioactivity release control guidelines would, in all events, have been previously initiated in response to other variables (e.g., RPV Water Level). This conclusion is reached because the source terms required to reach release rates associated with a general emergency (the point at which the emergency action is required by the EPG) can only occur following a release of a substantial proportion of the fuel noble gas inventory. Prevention of such a release is a primary goal of the RPV control guideline. Also, the other operator action (isolate lines discharging outside the primary and secondary containment) are intended to be taken at levels low enough as to not pose a significant risk for the general public. The primary lines

which communicate with the RPV are automatically isolated on high steamline radiation which satisfies the intent of the EPG action for these lines. Other lines which pass outside of the primary and secondary containment but which do not communicate directly with the RPV also receive automatic isolation signals. Thus, response to the radioactivity release control guideline is considered to be a contingency action and is not required to be Type A.

(2) General Variable Assessments

This section summarizes the results of the individual variable assessments concentrating on deviations identified between the existing design of the ABWR and the implementation position for Regulatory Guide 1.97 regarding the need for unambiguous indication.

Strict compliance with the regulatory guide is not provided in all cases. In some cases, an acceptable alternate has been proposed which meets the intent to have meaningful post-accident indications. For some parameters, this can be met by alternate variables to those specified in the Regulatory Guide 1.97 or by specifying combinations of other variables. Another approach chosen is to take exception to the guide where a reasonable justification can be provided.

(a) Drywell Pressure

Requirements for monitoring of drywell pressure are specified for both narrow range (from about -34.32 kPaG to + 34.32 kPaG) and wide range (from 0 to 110% of design pressure). The narrow range monitoring requirement is satisfied in the existing safety-related design by the four divisions of drywell pressure instruments which provide inputs to the initiation of the reactor protection (trip) system (RPS) and the emergency core cooling systems (ECCS). The requirement for unambiguous wide range drywell pressure monitoring are satisfied with two channels of drywell pressure instrumentation integrated with two channels of wetwell pressure instrumentation. Given the existence of (1) the normal pressure suppression vent path between the drywell and wetwell and (2) the wetwell to drywell vacuum breakers, the long-term pressure within the drywell and wetwell will be approximately the same. Therefore, if the two wide range drywell pressure indications disagreed, the operator could refer to the wetwell containment pressure indications to determine which of the two drywell pressure indications is correct. In order to provide full range pressure comparisons between the drywell wide range and wetwell pressure instruments, the drywell

pressure instrument range is 689.4 kPa. This value exceeds the required value of 110% of design pressure.

(b) Containment Pressure (Wetwell Pressure)

Requirements for monitoring of wetwell containment pressure specify the monitored range to be –34.32 kPaG to three times the design pressure for concrete containments. For the ABWR, 3 times the design pressure is about 931.6 kPaG. The ABWR primary containment has diaphragm safety devices which release wetwell atmosphere at about 617.8 kPaG. Therefore, it is not credible for containment pressure to achieve this value. For this reason and for better resolution of the measurements, the top of the instrument range for containment pressure is 689.4 kPaG. Two channels of instrumentation covering this full pressure range provide adequate post accident monitoring (PAM) indication of primary containment pressure since any disagreement between the output of the two channels could be resolved by the operator's reference to the drywell pressure indicators as discussed above. Since wetwell pressure is the parameter used by the control room operator to manually initiate wetwell spray, wetwell pressure is considered a Type A variable.

(c) Coolant Level in the Reactor

The RPV water level is the primary variable indicating the availability of adequate core cooling. Indication of water level by the differential pressure method is considered acceptable, (without diverse methods of sensing and indication), provided adequate redundancy for qualification of unambiguity is provided over the entire range of interest which extends from the bottom of the core support plate to the center line of the main steamlines.

In the ABWR design, the RPV water level wide range instruments and fuel zone instruments are utilized to provide this Post Accident Monitoring (PAM) indication. The four divisions of wide range instruments cover the range from above the core to the main steamlines. The two channels of fuel zone instruments cover the range from below the core to the top of the steam separator shroud.

Evaluation has concluded that two channels of fuel zone level instrumentation provide adequate post accident monitoring capability. Post-accident operator actions will be in accordance with detailed procedures developed based upon the Emergency Procedure Guidelines (EPG). In the event the vessel water level is below the range

of the wide range level (WRL) sensors (i.e., the water level is in the fuel zone range) and the two channels of fuel zone level instrumentation disagree, the EOPs instruct the operator to use the lower of the two and return the water level back up into the range of the WRL instrumentation. Using the four divisions of WRL instruments, an unambiguous indication of vessel water level can be determined, despite a postulated failure of a single instrument channel or division, and the operator could safely continue the execution of appropriate accident instigation activities as defined by the EOPS.

(d) BWR Core Temperature

Regulatory Guide 1.97 requires BWR core temperature (thermocouples) as a diverse indication of adequate core cooling. General Electric and the BWR Owners' Group have taken exception to this requirement for diverse indication based upon studies regarding the relationship between reactor water level and adequate core cooling. It is General Electric's view that no instrumentation other than RPV water level indication is required to assure indication of adequate core cooling.

(e) Drywell Sump Level

An exception is made to Regulatory Guide 1.97 as written for the design category for the equipment drain sump level. Rather than Category 1, General Electric considers the Category 3 design requirements to be more appropriate for the following reason: Indication of drywell floor drain sump level provides monitoring of leakage to the drywell and will be an early indication of a very small reactor coolant system leak/break for those events for which the drywell cooling system remains operable. However, it is primarily a backup variable to other indications of reactor coolant system leaks/breaks such as drywell pressure or drywell radiation level. In addition, containment water level is provided as a Type D, Category 2 variable. A lower design classification for drywell sump level is therefore appropriate and triplicated instrument channels are not necessary.

(f) Containment Area Radiation

The Containment Atmospheric Monitoring System (CAMS) consists of two independent and redundant radiation monitoring channels which provide indication of wetwell and drywell radiation levels. Emergency response actions regarding this variable are consistently directed toward minimizing the magnitude of this parameter. This two channel CAMS design provides adequate PAM indication since, in the event that the two

channels of information disagree, the operator can determine a correct and safe action based upon the higher of the two (in-range) indicators.

(g) Primary Containment Isolation Valve Position

The primary containment isolation valve position information provides indication to the operator regarding the successful completion of the primary containment isolation safety function. Following the requirements of 10CFR50 Appendix A, General Design Criteria 54, 55, 56 and 57, lines which penetrate the primary reactor containment are provided with varying degrees of redundant manual, check and automatically initiated isolation valves. Indication of the successful completion of the primary containment isolation safety function is provided by valve closed / not closed indicators for individual power operated valves. This arrangement, which provides redundant isolation valves and independent indication of valve position, is considered sufficient to satisfy the intent of Regulatory Guide 1.97 without requiring the use of triplicated instrument channels.

(h) Coolant Radiation

The indicator of coolant radiation leakage will be provided by the Process Radiation Monitoring System (PRMS) Main Steamline (MSL) radiation monitor subsystem. This subsystem consists of four physically and electrically separated and redundant divisions. Each division has a single channel consisting of a local radiation detection assembly, control room readout and trip actuators (Figure 7.6-5, sh 1). Each channel is located such that it can monitor each mainsteam line. These four divisions of PRMS radiation instrumentation satisfy the Regulatory Guide requirement for unambiguous indication.

(i) Suppression Pool Water Temperature

The ABWR Suppression Pool Temperature Monitoring (SPTM) System design requirements satisfy the Regulatory Guide 1.97 requirements regarding redundancy. The SPTM System is composed of four separate and independent instrument divisions. Each division has associated with it multiple thermocouples which are spatially distributed around the suppression pool. With this configuration, the bulk average suppression pool temperature can be determined even in the event of the loss of an entire division of instrumentation, since thermocouple sensors of each division will be located in close proximity to facilitate direct comparison. Although the ABWR design initiates reactor scram and suppression pool cooling automatically on high pool temperature, suppression pool water

temperature variable is considered a Type A variable since no credit is taken for automatic initiation in the safety analysis.

(j) Drywell Atmosphere Temperature

Surveillance monitoring of the temperatures in the drywell is provided by multiple temperature sensors distributed throughout the drywell to detect local area "hot-spots" and to monitor the operability of the drywell cooling system. With this drywell air temperature monitoring system supplied by multiple temperature sensors throughout the drywell, the Regulatory Guide 1.97 requirements for monitoring of drywell air temperature are met and provides the ability to determine drywell bulk average temperature.

(k) Drywell/Wetwell Hydrogen/Oxygen Concentration

The Containment Atmospheric Monitoring System (CAMS) consists of two independent and redundant drywell/containment oxygen and hydrogen concentration monitoring channels. Emergency response actions regarding these variables are consistently directed toward minimizing the magnitude of these parameters (i.e., there are no safety actions which must be taken to increase the hydrogen/oxygen levels if they are low). Consequently, the two channel CAMS design provides adequate PAM indication, since, in the event that the two channels of information disagree, the operator can determine a correct and safe action based upon the higher of the two (in-range) indications.

(l) Wetwell Atmosphere Air Temperature

Surveillance monitoring of temperatures in the wetwell is provided by multiple temperature sensors dispersed throughout the wetwell, therefore, the required indication of bulk average wetwell atmosphere temperature is satisfied.

(m) Standby Liquid Control System Flow

No flow indication is provided for the ABWR design. The positive displacement SLCS pumps are designed for constant flow. Any flow blockage or line break would be indicated by abnormal system pressure (high or low as compared to RCS pressure) following SLCS initiation. Changing neutron flux, SLCS pressure and SLCS tank level are substituted for SLCS flow and are considered adequate to verify proper system function. One channel of SLCS discharge pressure is provided in addition to the monitoring of neutron flux.

(n) Suppression Pool/Wetwell Water Level

Regulatory Guide 1.97 suggests two ranges for suppression pool water level (i.e., bottom of ECCS suction to 1.5m above normal water level and top of vent to top of weir wall [BWR 6, Mark III Containment]). The ABWR provides:

(i) Four (4) divisions of narrow range suppression pool water (e.g., approximately 0.5 meters above and below normal water level) for control of normal water level and automatic transfer of RCIC and HPCF suctions.

(ii) Two (2) wide range suppression pool/wetwell water level instruments from approximately the centerline of the ECCS suction piping to the wetwell spray spargers. This range allows for control of suppression pool/wetwell water level in the vicinity of the spray spargers at the high end and the ECCS pumps (vortex limits) at the low end.

Two (2) wide range wetwell level instruments are sufficient to control water level at the high level and at the low level by using the highest reading and the lowest reading instruments, respectively, should the instruments disagree. In addition, The low end measurement to the centerline of the ECCS suction piping is considered sufficient since this level measurement is low enough to allow control of the pump vortex limits.

(Note: See drywell water level for instrument range overlap).

(o) Drywell Water Level

The lower drywell water level measurement below the RPV (other than sump level) is not warranted because of its inability to survive a severe accident (core melt) and because of the following: When the suppression pool level is increased to accommodate severe accident drywell flooding (per the ABWR EPGs), suppression pool level will stop increasing while the water spills into the lower drywell through the vents. Once drywell and wetwell water levels equalize, the increase in drywell level will be monitored by the wetwell water level monitors up to the bottom of the RPV. (See also upper drywell water level monitoring for instrument overlap.)

In addition to the above discussion of lower drywell water level monitoring, the ABWR design provides for two (2) upper drywell water level monitors. The range of these instruments in from approximately 0.5 meters below the RPV (lower drywell and above wetwell to lower drywell vents) to the maximum primary containment water level limit

(MPCWLL) (upper drywell and approximately five (5) meters above TAF.). This lower range provides an approximately 0.5 meter instrument overlap with the wetwell water level instruments and therefore provides four (4) instruments for monitoring water immediately below the RPV during severe accident conditions.

Two (2) wide range upper drywell level measurements are sufficient, since there is sufficient margin between the TAF and MPCWLL to allow controlling water with the highest level measurement, should the instruments disagree, and still assure containment integrity and core coverage for containment flooding with no severe accident condition.

(p) Standby Liquid Control System Tank Level

As SLCS storage tank level is a backup variable to SLCS discharge pressure as described in the previous section (m), Category 3 qualification is appropriate instead of Category 2 suggested by Regulatory Guide 1.97.

## Table 7.5-1 Design and Qualification Criteria for Instrumentation

| Category 1 | Category 2 | Category 3 |
|---|---|---|
| 1. Equipment Qualification | | |
| The instrumentation is qualified in accordance with Regulatory Guide 1.89, "Qualification of Class 1E Equipment for Nuclear Power Plants", and the methodology described in NUREG-0588, "Interim Staff Position on Environmental Qualification of Safety-Related Electrical Equipment". | Same as Category 1 | No specific provision |
| (For equipment located in a mild environment, no specific environmental qualification is required except as required by General Design Criterion 4 of 10CFR50.) | (Same as Category 1) | (No specific provision) |
| Instrumentation whose ranges are required to extend beyond those ranges calculated in the most severe DBA event for a given variable are qualified using the guidance provided in Paragraph 63.6 of ANS-4.5. | Same as Category 1 | No specific provision |
| Qualification applies to the complete instrumentation channel from sensor to display where the display is a direct-indicating meter or recording device. If the instrumentation channel signal is used in a computer-based display, recording, or diagnostic program, qualification applies from the sensor up to and including the channel isolation device. | Same as Category 1 | No specific provision |
| The seismic portion of qualification is in accordance with Regulatory Guide 1.100, "Seismic Qualification of Electric Equipment for Nuclear Power Plants." Instrumentation should continue to read within the required accuracy following, but not necessarily during, a safe shutdown earthquake. | No specific provision | No specific provision |

## Table 7.5-1 Design and Qualification Criteria for Instrumentation (Continued)

| Category 1 | Category 2 | Category 3 |
|---|---|---|
| 2. Redundancy | | |
| No single failure within either the accident-monitoring instrumentation, its auxiliary supporting features, or its power sources concurrent with the failures that are a condition or result of a specific accident should prevent the operators from being presented the information necessary for them to determine the safety status of the plant and to bring the plant to and maintain it in a safe condition following that accident. Where failure of one accident-monitoring channel results in information ambiguity (that is, the redundant displays disagree) that could lead operators to defeat or fail to accomplish a required safety function, additional information should be provided to allow the operators to deduce the actual conditions in the plant. This is accomplished by providing additional independent channels of information of the same variable (addition of an identical channel) or by providing an independent channel to monitor a different variable that bears a known relationship to the multiple channels (addition of a diverse channel). Redundant or diverse channels are electrically independent and physically separated from each other and from equipment not classified important to safety in accordance with Regulatory Guide 1.75, “Physical Independence of Electric Systems,” up to and including any isolation device. Within each redundant division of a safety system, redundant monitoring channels are not needed except for steam generator level instrumentation in two-loop plants. | No specific provision | No specific provision |

## Table 7.5-1 Design and Qualification Criteria for Instrumentation (Continued)

| Category 1 | Category 2 | Category 3 |
|---|---|---|
| 3. Power Source | | |
| The instrumentation is energized from station standby power sources as provided in Regulatory Guide 1.32, "Criteria for Safety-Related Electric Power Systems for Nuclear Power Plants," and is backed up by batteries where momentary interruption is not tolerable. | The instrumentation is energized from a high-reliability power source, not necessarily standby power, and backed up by batteries where momentary interruption is not tolerable. | No specific provision |
| 4. Channel Availability | | |
| The instrumentation channel is available prior to an accident except as provided in Paragraph 4.11, "Exception," as defined in IEEE-279, 1971, "Criteria for Protection Systems for Nuclear Power Generating Stations," or as specified in the technical specifications. | The out-of-service interval is based on normal technical specification requirements on out-of-service for the system it serves where applicable or where specified by other requirements. | No specific provision |
| 5. Quality Assurance | | |
| The recommendations of the following regulatory guides pertaining to quality assurance are followed: | Same as Category 1 as modified by the following: | The instrumentation is of high-quality commercial grade and is selected to withstand the specific service environment. |
| Regulatory Guide 1.28 "Quality Assurance Program Requirements Design and Construction"<br>Regulatory Guide 1.30 (Safety Guide 30) "Quality Assurance Requirements for the Installation, Inspection, and Testing of Instrumentation and Electric Equipment" | Since some instrumentation is less important to safety than other instrumentation, it is not necessary to apply the same quality assurance measures to all instrumentation. The quality assurance requirements that are implemented provide control over activities affecting quality to an extent consistent with the importance to safety of the instrumentation. | |

## Table 7.5-1 Design and Qualification Criteria for Instrumentation (Continued)

| Category 1 | Category 2 | Category 3 |
|---|---|---|
| Regulatory Guide 1.38 "Quality Assurance Requirements for Packaging, Shipping Receiving, Storage and Handling of Items for Water-Cooled Nuclear Power Plants" | | |
| Regulatory Guide 1.58 "Qualification of Nuclear Power Plant Inspection, Examination, and Testing Personnel" | | |
| Regulatory Guide 1.64 "Quality Assurance Requirements for the Design of Nuclear Power Plants" | | |
| Regulatory Guide 1.74 "Quality Assurance Terms and Definitions" | | |
| Regulatory Guide 1.88 "Collection, Storage, and Maintenance of Nuclear Power Plant Quality Assurance Records" | | |
| Regulatory Guide 1.123 "Quality Assurance Requirements for Control of Procurement of Items and Services for Nuclear Power Plants" | | |
| Regulatory Guide 1.144 "Auditing of Quality Assurance Programs for Nuclear Power Plants" | | |
| Regulatory Guide 1.146 "Qualification of Quality Assurance Program Audit Personnel for Nuclear Power Plants" | | |
| 6. Display and Recording | | |
| Continuous real-time display is provided. The indication is on a dial, digital display, CRT, or strip-chart recorder. | The instrumentation signal is displayed on an individual instrument or it is processed for display on demand. | Same as Category 2 |
| Recording of instrumentation readout information is provided for at least one redundant channel. | Signals from effluent radioactivity monitors and area monitors are recorded. | Signals from effluent radioactivity monitors, and meteorology monitors are recorded. |

**Table 7.5-1 Design and Qualification Criteria for Instrumentation (Continued)**

| Category 1 | Category 2 | Category 3 |
|---|---|---|
| If direct and immediate trend or transient information is essential for operator information or action, the recording is continuously available on redundant dedicated recorders. Otherwise, it is continuously updated, stored in computer memory, and displayed on demand. Intermittent displays such as data loggers and scanning recorders are used if no significant transient response information is likely to be lost by such devices. | Same as Category 1 | Same as Category 1 |
| 7. Range | | |
| If two or more instruments are needed to cover a particular range, overlapping of instrument span is provided. If the required range of monitoring instrumentation results in a loss of instrumentation sensitivity in the normal operating range, separate instruments are used. | Same as Category 1 | Same as Category 1 |
| 8. Equipment Identification | | |
| [See also item 11] | | |
| Types A, B, and C instruments designated as Categories 1 and 2 are specifically identified with a common designation on the control panels so that the operator can easily discern that they are intended for use under accident conditions. | Same as Category 1 | No specific provision |
| 9. Interfaces | | |
| The transmission of signals for other use is through isolation devices that are designated as part of the monitoring instrumentation and that meet the provisions of this document. | Same as Category 1 | No specific provision |
| 10. Servicing, Testing, and Calibration | | |
| Servicing, testing, and calibration programs are specified to maintain the capability of the monitoring instrumentation. If the required interval between testing is less than the normal time interval between plant shutdowns, a capability for testing during power operation is provided. | Same as Category 1 | Same as Category 1 |

## Table 7.5-1 Design and Qualification Criteria for Instrumentation (Continued)

| Category 1 | Category 2 | Category 3 |
|---|---|---|
| Whenever means for removing channels from service are included in the design, the design facilitates administrative control of the access to such removal means. | Same as Category 1 | Same as Category 1 |
| The design facilitates administrative control of the access to all setpoint adjustments, module calibration adjustments, and test points. | Same as Category 1 | Same as Category 1 |
| Periodic checking, testing, calibration and calibration verification are in accordance with the applicable portions of Regulatory Guide 1.118, "Periodic Testing of Electric Power and Protection Systems," pertaining to testing of instrument channels. (Note: Response time testing not usually needed.) | Same as Category 1 | Same as Category 1 |
| The location of the isolation device is such that it would be accessible for maintenance during accident conditions. | Same as Category 1 | No specific provision |
| 11. Human Factors<br>[See also item 8] | | |
| The instrumentation is designed to facilitate the recognition, location, replacement, repair, or adjustment of malfunctioning components or modules. | Same as Category 1 | Same as Category 1 |
| The monitoring instrumentation design minimizes the development of conditions that would cause meters, annunciators, recorders, alarms, etc., to give anomalous indications potentially confusing to the operator. Human factors analysis is used in determining type and location of displays (see Chapter 18). | Same as Category 1 | Same as Category 1 |
| To the extent practicable, the same instruments are used for accident monitoring as are used for the normal operations of the plant to enable the operators to use, during accident situations, instruments with which they are most familiar. | Same as Category 1 | Same as Category 1 |

## Table 7.5-1 Design and Qualification Criteria for Instrumentation (Continued)

| Category 1 | Category 2 | Category 3 |
|---|---|---|
| 12. Direct Measurement<br>To the extent practicable, monitoring instrumentation inputs are from sensors that directly measure the desired variables. An indirect measurement is made only when it can be shown by analysis to provide unambiguous information. | Same as Category 1 | Same as Category 1 |

## Table 7.5-2 ABWR PAM Variable List

| Variable | Range Required | Type | Category | Discussion Section |
|---|---|---|---|---|
| Neutron Flux | $10^{-6}$% to 100% full power | B | 1 | |
| Control Rod Position | Full in or not full in | B | 3 | |
| Boron Concentration | 0–1000 ppm | B | 3 | |
| BWR Core Temperature | 93.3°C to 1260°C | | | Subsection 7.5.2.1(2)(d) |
| Reactor Coolant System Pressure | 0 to10.35 MPaG | B,C,D | 1 | |
| Drywell Pressure | 0.034 MPaG to 0.021 MPaG (narrow range) 0–100% design pressure (wide range) | B,C,D | 1 | Subsection 7.5.2.1(2)(a) |
| Drywell Sump Level | Top to Bottom | B,C | 3 | Subsection 7.5.2.1(2)(e) |
| Coolant Level in Reactor | Bottom of core plate to main steamline | B,C | 1 | Subsection 7.5.2.1(2)(c) |
| Suppression Pool Water Level | Bottom of ECCS suction line to 1.5 meters above normal water line | C | 1 | Subsection 7.5.2.1(2)(n) |
| | Top of vent to top of weir wall | D | 2 | Subsection 7.5.2.1(2)(n) |
| Drywell Water Level | (None specified) | D | 2 | Subsection 7.5.2.1(2)(o) |
| Containment Area Radiation | $10^{-2}$ Gy/h to $10^{5}$Gy/h | C,E | 1 | Subsection 7.5.2.1(2)(f) |
| Wetwell Pressure | – 0.034 MPaG to 3 times design pressure | A,B,C | 1 | Subsection 7.5.2.1(2)(b) |
| Primary Containment Isolation Valve Position | Closed – not closed | B | 1 | Subsection 7.5.2.1(2)(g) |
| Coolant Gamma | 370 μBq to 370Bq/ml or TID-14844 Source Term in Coolant Volume | C | 3 | |
| Coolant Radiation | 1/2 Tech Spec limit to 100 times Tech Spec limit | C | 1 | Subsection 7.5.2.1(2)(h) |
| RHR Flow | 0–110% Design Flow | D | 2 | |
| HPCF Flow | 0–110% Design Flow | D | 2 | |
| RHR Heat Exchanger Outlet Temperature | 4.4°C to 176.7°C | D | 2 | |
| RCIC Flow | 0–110% Design Flow | D | 2 | |
| Standby Liquid Control System Flow | 0–110% Design Flow | D | 2 | Subsection 7.5.2.1(2)(m) |

## Table 7.5-2 ABWR PAM Variable List (Continued)

| Variable | Range Required | Type | Cate-gory | Discussion Section |
|---|---|---|---|---|
| SLCS Storage Tank Level | Top to Bottom | D | 3 | Subsection 7.5.2.1(2)(o) |
| SRV Position | Closed – Not Closed | D | 2 | |
| Feedwater Flow | 0–110% Design Flow | D | 3 | |
| High Radioactivity Liquid Tank Level | Top to Bottom | D | 3 | |
| Standby Energy Status | Plant Specific | D | 2 | |
| Suppression Pool Water Temperature | 4.4°C to 140°C | A, D | 1 | Subsection 7.5.2.1(2)(i) |
| Drywell Atmosphere Temperature | 4.4°C to 226.7°C | D | 1 | Subsection 7.5.2.1(2)(j) |
| Drywell/Wetwell Hydrogen Concentration | 0–30 Volume% | C | 1 | Subsection 7.5.2.1(2)(k) |
| Drywell/Wetwell Oxygen Concentration | 0–10 Volume% | C | 1 | Subsection 7.5.2.1(2)(k) |
| Wetwell Atmosphere Temperature | 4.4°C to 226.7°C | D | 1 | Subsection 7.5.2.1(2)(l) |
| Secondary Containment Airspace (effluent) Radiation Noble Gas | 37 pBq/$cm^3$ to 37MBq/$cm^3$ | C | 2 | |
| Containment Effluent Radioactivity—Noble Gas | 37 pBq/$cm^3$ to 0.37μBq/$cm^3$ | C | 3 | |
| Condensate Storage Tank Level | Top to Bottom | D | 3 | |
| Cooling Water Temperature to ESF System Components | 4.4°C to 93.3°C | D | 2 | |
| Cooling Water Flow to ESF System Components | 0–110% Design Flow | D | 2 | |
| Emergency Ventilation Damper Position | Open – Closed Status | D | 2 | |
| Service Area Radiation Exposure Rate | $10^{-3}$ Gy/h to $10^2$ Gy/h | E | 3 | |
| Purge Flows—Noble Gases and Vent Flow Rate | 37 PBq/$cm^3$ to 0.37 Bq/$cm^3$<br>0–110% Vent Design Flow | E | 2 | |
| Identified Release Points—Particulates and Halogens | 37 nBq/$cm^3$ to 3.7 mBq/$cm^3$<br>0–110% Vent Design Flow | E | 3 | |

## Table 7.5-2 ABWR PAM Variable List (Continued)

| Variable | Range Required | Type | Category | Discussion Section |
|---|---|---|---|---|
| Airborn Radiohalogens and Particulates | 37 $\mu$Bq/cm$^3$ to 37Bq/cm$^3$ | E | 3 | |
| Plant and Environs Radiation/Radioactivity (Portable Instruments) | $10^{-5}$ Gy/h to$10^2$ Gy/h photons $10^{-5}$ Gy/h to $10^2$ Gy/h, beta and low energy photons | E | 3 | Portable Instruments * |
| Meteorological Data (Wind Speed, Wind Direction, and Atmospheric Stability) | 0–360°<br>0–9.8 m/s | E | 3 | * |
| On Site Analysis Capability (Primary Coolant, Sump and Space Containment Air Grab Sampling) | Refer to Regulatory Guide 1.97 | E | 3 | * |
| Secondary Containment Area Temperature | | E | 2 | |
| Secondary Containment Area Radiation | $10^{-3}$ Gy/h to $10^2$ Gy/h | E | 2 | |

* Out of ABWR Standard Plant Scope

## Table 7.5-3 ABWR Type A Variables

| |
|---|
| Suppression Pool Water Temperature |
| Wetwell Pressure |

## Table 7.5-4 Anticipated Operational Transients

| Event Description | NSOA Event Figure No. | Tier 2 Section No. | Manual Action Variables* |
|---|---|---|---|
| Manual or Inadvertent SCRAM | 15A.6-7 | 15A.6.3.3 Event 7 | $P_{RPV}$, $L_{RPV}$ |
| Loss of Plant Instrument Service Air Systems | 15A.6-8 | 15A.6.3.3 Event 8 | $T_{SP}$,$P_{RPV}$, $L_{RPV}$ |
| Recirculation Flow Control Failure—One RIP Runout | 15A.6-9 | 15.4.5 | $P_{RPV}$, $L_{RPV}$ |
| Recirculation Flow Control Failure—One RIP Runback | 15A.6-10 | 15.3.2 | $P_{RPV}$, $L_{RPV}$ |
| Three RIPs Trip | 15A.5-11 | 15.3.1 | $P_{RPV}$, $L_{RPV}$ |
| All MSIV Closure | 15A.6-12 | 15.2.4 | $T_{SP}$,$P_{RPV}$, $L_{RPV}$ |
| One MSIV Closure | 15A.6-13 | 15.2.4 | $T_{SP}$,$P_{RPV}$, $L_{RPV}$ |
| Loss of All Feedwater Flow | 15A.6-14 | 15.2.7 | $P_{RPV}$, $L_{RPV}$ |
| Loss of a Feedwater Heater | 15A.6-15 | 15.1.1 | $\phi$,$P_{RPV}$, $L_{RPV}$ |
| Feedwater Controller Failure—Runout of One Feedwater Pump | 15A.6-16 | 15.1.2 | $P_{RPV}$, $L_{RPV}$ |
| Pressure Regulator Failure—Opening of One Bypass Valve | 15A.6-17 | 15.1.3 | $P_{RPV}$, $L_{RPV}$ |
| Pressure Regulator Failure—Opening of One Control Valve | 15A.6-18 | 15.2.1 | $P_{RPV}$, $L_{RPV}$ |
| Main Turbine Trip with Bypass System Operational | 15A.6-19 | 15.2.3 | $T_{SP}$, $P_{RPV}$, $L_{RPV}$ |
| Loss of Main Condenser Vacuum | 15A.6-20 | 15.2.5 | $P_{RPV}$, $L_{RPV}$ |
| Generator Load Rejection with Bypass System Operational | 15A.6-21 | 15.2.2 | $T_{SP}$,$P_{RPV}$,$L_{RPV}$ |
| Loss of Unit Auxiliary Transformer | 15A.6-22 | 15.2.6 | $T_{SP}$,$P_{RPV}$, $L_{RPV}$ |

* See Table 7.5-9 for Definition of symbols

## Table 7.5-5 Abnormal Operational Transients

| Event Description | NSOA Event Figure No. | Tier 2 Section No. | Manual Action Variables* |
|---|---|---|---|
| Inadvertent Startup of HPCF Pump | 15A.6-23 | 15.5.1 | $\phi$ |
| Inadvertent Opening of a Safety/Relief Valve | 15A.6-24 | 15.1.4 | $T_{SP}$,$P_{RPV}$,$L_{RPV}$ |
| Control Rod Withdrawal Error—Startup and Refueling Operations | 15A.6-25 | 15.4.1 | $\phi$ |
| Main Turbine Trip with One Bypass Valve Failure | 15A.6-26 | 15.2.3 | $T_{SP}$,$P_{RPV}$,$L_{RPV}$ |
| Generator Load Rejection with One Bypass Valve Failure | 15A.6-27 | 15.2.2 | $T_{SP}$,$P_{RPV}$,$L_{RPV}$ |

* See Table 7.5-9 for Definition of Symbols

## Table 7.5-6 Design Basis Accidents

| Event Description | NSOA Event Figure No. | Tier 2 Section No. | Manual Action Variables* |
|---|---|---|---|
| Control Rod Ejection Accident | 15A.6-28 | 15.4.8 | None† |
| Control Rod Drop Accident | 15A.6-29 | 15.4.9 | $P_{RPV}, L_{RPV}, \phi$ |
| Control Rod Withdrawal Error Power Operation | 15A.6-30 | 15.4.2 | None† |
| Fuel Handling Accident | 15A.6-31 | 15.7.4 | $R_{2C}$ |
| Loss-of-Coolant Accident Resulting from Spectrum of Postulated Piping Breaks within the RCPB Inside Containment | 15A.6-32 | 15.6.5 | $H_{2C}, O_{2C}, L_{RPV}, L_{SP}, P_{RPV}, P_{DW}$ Ø |
| Small, Large, Steam and Liquid Piping Breaks Outside Containment | 15A.6-33 | 15.6.4 | $T_{SP}, P_{RPV}, L_{RPV}$ |
| Abnormal Startup of Idle Reactor Internal Pump | 15A.6-38 | 15.4.4 | $P_{RPV}, L_{RPV}$ |
| Recirculation Flow Control Failure—All RIPs Runout | 15A.6-39 | 15.4.5 | Ø, $L_{RPV}$ |
| Recirculation Flow Control Failure—All RIPs Runback | 15A.6-40 | 15.3.2 | $L_{RPV}$ |
| Trip of All RIPs | 15A.6-41 | 15.3.1 | $P_{RPV}, L_{RPV}$ |
| Loss of RHR Shutdown Cooling | 15A.6-42 | 15.2.9 | $T_{RPV}$ |
| RHR Shutdown Cooling Increased Cooling | 15A.6-43 | 15.1.6 | $T_{RPV}$ |
| Feedwater Controller Failure Runout of Two Feedwater Pumps | 15A.6-44 | 15.1.2 | $P_{RPV}, L_{RPV}$ |
| Pressure Regulatory Failure—Opening of All Bypass and Control Valves | 15A.6-45 | 15.1.3 | $P_{RPV}, L_{RPV}$ |
| Pressure Regulatory Failure—Closure of All Bypass and Control Valves | 15A.6-46 | 15.2.1 | $T_{SP}, P_{RPV}, L_{RPV}$ |
| Main Turbine Trip with Bypass Failure | 15A.6-48 | 15.2.3 | $T_{SP}, P_{RPV}, L_{RPV}$ |
| Generator Load Rejection with Bypass Failure | 15A.6-49 | 15.2.2 | $T_{SP}, P_{RPV}, L_{RPV}$ |
| Misplaced Fuel Bundle Accident | 15A.6-50 | 15.4.7 | None |
| Reactor Internal Pump Seizure | 15A.6-51 | 15.3.3 | $P_{RPV}, L_{RPV}$ |
| Reactor Internal Pump Shaft Break | 15A.6-52 | 15.3.4 | $P_{RPV}, L_{RPV}$ |

* See Table 7.5-9 for Definition of Symbols.

† Analysis indicates not plausible.

## Table 7.5-7 Special Events

| Event Description | NSOA Event Figure No. | Tier 2 Section No. | Manual Action Variables* |
|---|---|---|---|
| Shipping Cask Drop Spent Fuel | 15A.6-53 | 15.7.5 | None |
| Reactor Shutdown From Anticipated Transient Without SCRAM (ATWS) | 15A.6-54 | 15.8 | $T_{SP}$,$P_{RPV}$,$L_{RPV}$, $P_{DW}$ |
| Reactor Shutdown from Outside Control Room | 15A.6-55 | 15A.6.6.3 | $T_{SP}$,$L_{SP}$,$L_{RPV}$,$P_{RPV}$ Event 55 |
| Reactor Shutdown Without Control Rods | 15A.6-56 | 15A.6.6.3 | $T_{SP}$,$\phi$,$L_{RPV}$,$P_{RPV}$ Event 56 |

* See Table 7.5-9 for Definition of Symbols.

## Table 7.5-8 Summary of Manual Actions

| Manual Action | Variable* | Source† |
|---|---|---|
| Decrease Reactor Power | $\phi$ | T |
| Initiation of Suppression Pool Cooling | $T_{SP}$ | T |
| Initiation of Shutdown Cooling | $P_{RPV}$,$L_{RPV}$ | T |
| Manual Depressurization | $P_{RPV}$,$L_{RPV}$ | T |
| Initiation of $N_2$ Make Up and Purge | $H_{2C}$,$O_2$ | T |
| Initiation of Leakage Control Systems | N/A for ABWR | N/A for ABWR |
| Initiate Standby Liquid Control | $\phi$,$T_{SP}$ | T |
| Lowering Power by Lowering Water Level (ATWS) | $\phi$,$L_{RPV}$ | E |
| Emergency Action‡ If Exceed: | | E |
| Heat Capacity Temperature Limit | $T_{SP}$,$P_{RPV}$ | |
| Heat Capacity Level Limit | $T_{SP}$,$L_{SP}$ | |
| Suppression Pool Load Limit | $L_{SP}$,$P_{RPV}$ | |
| Reference Leg Boiling Limit | $T_{DW}$,$T_{RPV}$ (or $P_{RPV}$) | |
| SRV Tailpipe Level Limit | $L_{SP}$,$P_{RPV}$ | |
| Maximum Primary Containment Water Level Limit | Lc ,$P_{WW}$ | |
| Maximum Drywell Temperature | $T_{DW}$ | |
| Maximum Containment Temperature | $P_{WW}$,$L_{SP}$ | |
| Maximum Containment Pressure | $P_{WW}$,$L_{SP}$ | |
| Pressure Suppression Limit | $P_{WW}$,$L_{SP}$ | |
| Maximum Secondary Containment Operating Valves | $T_{2C,}R_{2C,}L_{2C}$ | |
| Offsite Release Rate | $R_E$ | |
| Initiation of Drywell/Wetwell Sprays | $T_{DW}$,$T_{WW}$,$P_{DW}$,$L_{SP}$ | E |
| Initiation of Containment Flooding | $P_{RPV}$,$L_{RPV}$ | |
| Initiation of RPV Venting | $P_{RPV}$,$L_{RPV}$ | |
| Terminate Containment Flooding | Rc, $L_{RPV}$, Lc | |

* See Table 7.5-9 for Definition of Symbols.

† E = EPG; T = Tier 2

‡ Scram, Emergency RPV Depressurization, RPV Flooding and/or Drywell Cooling.

## Table 7.5-9 Definition of Symbols for Tables 7.5-4 Through 7.5-8

| | | |
|---|---|---|
| $T_{SP}$ | — | Suppression Pool Temperature |
| $T_{DW}$ | — | Drywell Temperature |
| $T_{RPV}$ | — | Reactor Water Temperature |
| $P_{RPV}$ | — | RPV Pressure |
| $P_{WW}$ | — | Wetwell Pressure |
| $L_{RPV}$ | — | RPV Level |
| $L_{SP}$ | — | Suppression Pool Level |
| Ø | — | Neutron Flux |
| $H_{2C}$ | — | Drywell/Wetwell Hydrogen Concentration |
| $O_{2C}$ | — | Drywell/Wetwell Oxygen Concentration |
| $P_{DW}$ | — | Drywell Atmospheric Pressure |
| $T_{2C}$ | — | Temperature—Secondary Containment |
| $R_{2C}$ | — | Radiation Level—Secondary Containment |
| $L_{2C}$ | — | Sump Level—Secondary Containment |
| $R_E$ | — | Exhaust Vent Radiation Level |
| $L_C$ | — | Drywell Level |
| $R_C$ | — | Radiation Level-Primary Containment |

# 7.6 All Other Instrumentation Systems Required for Safety

## 7.6.1 Description

This section will examine and discuss the instrumentation and control aspects of the following plant systems:

- Neutron Monitoring System (SRNM, LPRM, and APRM)
- Process Radiation Monitoring System
- HP/LP interlocks
- Drywell Vacuum Relief System (Chapter 6)
- Containment Atmosphere Monitoring System
- Suppression Pool Temperature Monitoring System

A number of observations are cited relative to the evaluation of the instrumentation and control (I&C) portions of the subject systems:

(1) The systems themselves and their I&C portion serve design bases that are both safety and power generation.

(2) Some systems inherently perform mechanical or containment safety functions but need little I&C protective support.

(3) Some systems provide protective functions in selective minor events and are not required for other major plant occurrences.

(4) Some systems have only a small portion of their I&C participating in safety functions.

(5) The HP/LP interlocks in this section are an integral part of various modes of the RHR System functions described in other sections.

(6) A system/safety function, qualitative-level nuclear safety operational analysis (NSOA) is presented in Chapter 15. The interrelated design bases of the various safety system functions are also analyzed in this chapter.

### 7.6.1.1 Neutron Monitoring System-Instrumentation and Controls

The Neutron Monitoring System (NMS) consists of various safety-related subsystems: Startup Range Neutron Monitor (SRNM), Local Power Range Monitor (LPRM), and Average Power Range Monitor (APRM) subsystems. The non-safety-related ATIP and

MRBM Subsystems of the NMS are discussed in Section 7.7. The LPRM and the APRM, together, are also called the Power Range Neutron Monitor (PRNM).

(1) System Identification

The purpose of the Neutron Monitoring System (NMS) is to monitor power generation and, for the safety function part of the NMS, to provide trip signals to the Reactor Protection System (RPS) to initiate reactor scram under excessive neutron flux (and power) increase condition (high level) or neutron flux fast rising (short period) condition. The NMS also provides power information of operation and control of the reactor to the Plant Process Computer System (PCS) and the rod block monitor. A block diagram showing a typical NMS division is shown in Figure 7.6-4a. The operating ranges of the various detectors are shown in Figure 7.6-4b.

(2) System Safety Classification

The SRNM and PRNM (includes LPRM and APRM) Subsystems provide a safety function, and have been designed to meet the applicable design criteria.

The NMS is classified as shown in Table 3.2-1. The safety-related subsystems are qualified in accordance with Sections 3.10 and 3.11.

The ATIP and MRBM Subsystems of the NMS are non-safety-related and are discussed in Section 7.7.

(3) Power Sources

The power sources for each system are discussed in the individual circuit descriptions.

#### 7.6.1.1.1 Startup Range Neutron Monitor Subsystem—Instrumentation and Controls

(1) General Description

The startup range neutron monitor (SRNM) monitors neutron flux from the source range (1.E+3 neutron/$cm^2$) to 15% of the rated power. The SRNM Subsystem has 10 SRNM channels, each having one fixed in-core regenerative fission chamber sensor (Figures 7.6-1 and 7.6-2).

(2) Power Sources

SRNM channels are powered as listed below:

| Channels | | |
|---|---|---|
| A,E,J | 120 VAC UPS | Bus A (Division I) |
| B,F | 120 VAC UPS | Bus B (Division II) |
| C,G,L | 120 VAC UPS | Bus C (Division III) |
| D,H | 120 VAC UPS | Bus D (Division IV) |

Loss of a power supply bus will cause the loss of the SRNM channels in a division, but will result in loss of only one division of instrumentation.

(3) Physical Arrangement

The 10 detectors are all located at fixed elevation slightly above the midplane of the fuel region, and are evenly distributed throughout the core. The SRNM locations in the core, together with the neutron source locations, are shown in Figure 7.6-1. Each detector is contained within a pressure barrier dry tube inside the core, with signal output exiting the bottom of the dry tube undervessel. Detector cables then penetrate the primary containment and are connected to preamplifiers located in the Reactor Building. The SRNM preamplifier signals are then transmitted to the SRNM DMC (digital measurement and control) units in the control room. The DMC units provide algorithms for signal processing, flux, and power calculations, period trip margin and period calculations, and provide various outputs for local and control console displays, recorder, and to the plant process computer system. There are also the alarm and trip digital outputs for both high flux and short period conditions, and the instrument inoperative trip to be sent to the RPS and RCIS separately. The electronics for the SRNMs and their bypasses are located in four separate cabinets.

(4) Signal Processing

Over the 10-decade power monitoring range, two monitoring methods are used: (1) for the lower ranges the counting method which covers from 1.E+3 neutron/$cm^2$ to 1.E+9 neutron/$cm^2$, and (2) for the higher ranges, the Campbelling technique (mean square voltage, or MSV) which covers from 1.E+8 neutron/$cm^2$ to 1.E+13 neutron/$cm^2$ of neutron flux. In the counting range, the discrete pulses produced by the sensors are applied to a

discriminator after preamplification. The discriminator, together with other digital noise-limiter features, separates the neutron pulses from gamma radiation and other noise pulses. The neutron pulses are then counted. The reactor power is proportional to the count rate. In the MSV range, where it is difficult to distinguish the pulses, a DC voltage proportional to the mean square value of the input signal is produced. The reactor power is proportional to this mean square voltage. In the mid-range overlapping region, where the two methods are changed over, the DMC-based SRNM calculates the neutron flux based on a weighted interpolation of the two flux values calculated by both methods. A continuous and smooth flux reading transfer is achieved in this manner. There is also the calculation algorithm of the period-based trip circuitry that generates trip margin setpoint for the period trip protection function.

(5) Trip Functions

The SRNM scram trip functions are discussed in Section 7.2; rod block trip functions are discussed in Subsection 7.7.1.2. The SRNM channels also provide trip signals indicating when a SRNM channel is upscale, down-scale, inoperative, or bypassed. The SRNM trips are shown in Table 7.6-1.

(6) Bypasses and Interlocks

The 10 SRNM channels are divided into three bypass groups. With such bypass grouping, up to three SRNM channels can be bypassed at any time, with any one channel from each bypass group bypassed. There is no additional SRNM bypass capability at the divisional level. If a SRNM divisional out of service is required, this will generate a half trip to the RPS. For SRNM calibration or repair, the bypass can be done for each individual channel separately. There are separate bypass functions for the SRNM and the APRM in the NMS (i.e., there is no single NMS divisional bypass which will affect both the SRNM and the APRM). Any APRM bypass will not force a SRNM bypass. The SRNM and APRM bypasses are separate logics to the RPS, each interfacing with the RPS independently. Also, all NMS bypass logic control functions are located within the NMS, not in the RPS. The SRNM bypass switches are mounted on the control room panel.

The SRNM also sends an interlock signal to the safety system logic control (SSLC) system. This signal is called “ATWS Permissive” and is a binary signal indicating whether the SRNM power level is above or below a specific setpoint level (Table 7.6-1). If this signal is a “high” level indicating the power is above the setpoint, this will allow the SSLC to permit ATWS protection action such as permission to inject liquid poison.

(7) Redundancy and Diversity

The 10 SRNM channels are arranged into four divisions such that each of the four RPS divisions receives input signals from each and all of the four SRNM divisions. Failure of a single SRNM channel, once bypassed, will not cause a trip to the RPS. Such failure will not prevent proper operation of the remaining trip channels in performing their safety functions (Subsection 7.2.1.1.4.2 (1)).

(8) Testability

Each SRNM channel is tested and calibrated using the procedures listed in the SRNM instruction manual. Each SRNM channel can be checked to ensure that the SRNM high flux and period scram functions are operable.

(9) Environmental Considerations

The wiring, cables, and connectors located within the drywell are designed for continuous duty in the conditions described in Section 3.11.

The SRNM preamplifiers which are located in the Reactor Building, and the monitors, which are located in the control room, are designed to operate under design basis normal and abnormal conditions in those areas. The SRNM System components are designed to operate during and after certain design basis events such as earthquakes, accidents, and anticipated operational occurrences. Environmental qualification is discussed in Section 3.11.

(10) SRNM Operational Considerations

The SRNM has no special operating considerations.

#### 7.6.1.1.2 Power Range Neutron Monitor Subsystem—Instrumentation and Controls

The PRNM Subsystem consists of a Local Power Range Monitor (LPRM) Subsystem and an Average Power Range Monitor (APRM) Subsystem.

##### 7.6.1.1.2.1 Local Power Range Neutron Monitor Subsystem—Instrumentation and Controls

(1) General Description

The local power range monitor (LPRM) monitors local neutron flux in the power range. The LPRM provides input signals to the APRM Subsystem (Subsection 7.6.1.1.2.2) and to the plant computer system (Subsection 7.7.1.5). See Figures 7.6-1 and 7.6-2.

(2) Uninterruptible Power Supply (UPS)

Alternating-current (AC) power for the LPRM circuitry is supplied by four 120 VAC uninterruptible power supply (UPS) buses A, B, C, and D. Each bus supplies approximately one fourth of the detectors.

Each LPRM detector has a DC power supply in each division which furnishes the detector polarizing potential.

(3) Physical Arrangement

The LPRM Subsystem consists of 52 detector assemblies, each assembly consisting of four fission chamber detectors evenly spaced at four axial positions along the fuel bundle vertical direction. The assemblies are distributed throughout the whole core in evenly spaced locations such that each assembly is located at every fourth intersection of the water channels around fuel bundles not containing a control rod blade. The LPRM detector location is illustrated in Figure 7.6-3.

The LPRM detector is a fission chamber with a polarizing potential of approximately 100 VDC. The four detectors comprising a detector assembly are contained in a common tube that houses the automatic traversing in-core probe (ATIP) calibration tube. The enclosing housing tube contains holes to allow coolant flow for detector cooling. The whole assembly is installed or removed from the top of the reactor vessel, with the reactor vessel head removed. It is referred to as the top entry LPRM assembly. The upper end of the assembly is held under the top fuel guide plate with a spring plunger. A permanently installed in-core guide tube and housing is located below the lower core plate to confine the assembly and to provide a sealing surface under the reactor vessel.

(4) Signal Processing

The LPRM detector outputs are connected by coaxial cables from under the vessel pedestal region and routed through the primary containment penetration, and through the Reactor Building to be processed for signal conditioning analog-to-digital conversion function in the control room. The LPRM signals are connected to the APRM units in the control room, where the signals are amplified. Such amplified voltage is proportional to the local neutron flux level. The LPRM signals are then used by the APRM to produce APRM signals. The 208 LPRM detectors are separated and divided into four groups to provide four independent APRM signals. Individual LPRM signals are also transmitted through dedicated interface units (for isolation) to various systems such as the RCIS, and the plant process computer.

(5) Trip Functions

The LPRM channels provide alarm signals indicating when an LPRM is upscale, down-scale, or bypassed. However, such signals are not sent to the RPS for scram trip or RCIS for rad block.

(6) Bypasses and Interlocks

Each LPRM channel may be individually bypassed. When the maximum allowed number of bypassed LPRMs associated with any APRM channel has been exceeded, an inoperative trip is generated by that APRM.

(7) Redundancy

The LPRM detector assemblies are divided into groups. The redundancy criteria are met in the event of a single failure under permissible APRM bypass conditions. A scram signal can be generated in the Reactor Protection System (RPS) as required if the inoperative trip of the APRM is generated as described in (6).

(8) Testability

LPRM channels are calibrated using ATIP and data from previous full-power runs, and are tested using procedures in the applicable instruction manual.

(9) Environmental Considerations

The detector and detector assembly are designed to operate up to 8.27 MPaG at an ambient temperature of 302°C. The wiring, cables, and connector located within the drywell are designed for continuous duty. The LPRMs are capable of functioning during and after certain design basis events, including earthquakes and anticipated operational occurrences (Sections 3.10 and 3.11).

(10) Operational Considerations

The LPRM is a monitoring system with no special operating considerations.

#### 7.6.1.1.2.2 Average Power Range Monitor Subsystem—Instrumentation and Controls

The Average Power Range Monitor (APRM) includes the Oscillation Power Range Monitor (OPRM).

(1) General Description

(a) Average Power Range Monitor (APRM)

The APRMs are safety-related systems. There are four divisions of DMC-based APRM channels located in the control room. Each channel receives 52 LPRM signals as inputs, and averages such inputs to provide a core average neutron flux that corresponds to the core average power. One APRM channel is associated with each trip system of the Reactor Protection System (RPS). However, a trip signal from each APRM division also goes to all other RPS divisions, with proper signal isolation.

(b) Oscillation Power Range Monitor (OPRM)

The OPRM is a functional subsystem of the APRM. There are four safety-related OPRM channels, with each OPRM channel as part of each of the four APRM channels. Each OPRM receives the identical LPRM signals from the corresponding APRM channel as inputs, and forms a special OPRM cell configuration to monitor the neutron flux behavior of all regions of the core. Each OPRM cell represents a combination of four LPRM signals selected from the LPRM strings at the four corners of a four-by-four fuel bundle square region. The OPRM detects thermal hydraulic instability and provides trip functions to the RPS to suppress neutron flux oscillation prior to the violation of safety thermal limits. The OPRM trips are combined with the APRM trips of the same APRM channel, to be sent to the RPS.

(2) Power Sources

APRM channels are powered as listed below:

| Channels | | |
|---|---|---|
| A | 120 VAC UPS | Bus A (Division I) |
| B | 120 VAC UPS | Bus B (Division II) |
| C | 120 VAC UPS | Bus C (Division III) |
| D | 120 VAC UPS | Bus D (Division IV) |

The trip units and LPRM channels as well as the OPRM channel associated with each APRM channel receive power from the same power supply as the APRM channel.

(3) Signal Conditioning

(a) APRM

APRM channel electronic equipment averages the output signals from a selected set of LPRMs. The averaging circuit automatically corrects for the number of unbypassed LPRM amplifiers providing input signals.

Assignment of LPRMs to the APRM channels is shown in Figure 7.6-1. The LPRM detector in the bottom position of a detector assembly is designated Position A. Detectors above A are designated B and C, and the uppermost detector is designated D.

Reactor core flow signals derived from core plate pressure drop signals are used in the APRM to provide the flow biasing for the APRM rod block and thermal power trip setpoint functions. There is also the Core Flow Rapid Coastdown trip logic in the APRM unit which utilizes the core flow and thermal power information. The core flow signal is also used to provide the flow biassing for the MRBM rod block setpoint functions.

(b) OPRM

The OPRM utilizes the same set of LPRM signals used by the APRM that this OPRM channel resides with. Assignment of LPRMs to the four OPRM channels is identical to that referred to in Figure 7.6-1 which shows the assignment of LPRMs to APRM channels. Figure 7.6-13 shows the detailed LPRM assignments to the four OPRM channels, including the assignment of LPRMs to the OPRM cells. With this configuration, each OPRM cell receives four LPRM inputs from four LPRM strings at the four corners of the 4X4 fuel bundle square. For locations near the periphery where one corner of the square does not include an LPRM string, the OPRM cells use the inputs from the remaining three LPRM strings. The overall axial and radial distribution of these LPRMs between the OPRM channels are uniform. Each OPRM cell has four LPRMs from all four different elevations in the core. LPRM signals may be input to more that one OPRM cell within an OPRM channel. The LPRM signals assigned to each cell are summed and averaged to provide an OPRM signal for this cell.

The OPRM trip protection algorithm consists of trip logic depending on signal oscillation magnitude an signal oscillation period. For each cell, the peak to average value of the OPRM signal is determined to evaluate the magnitude of oscillation and to be used in the setpoint algorithm. The OPRM signal sampling and computation frequency is well above the

expected thermal-hydraulic oscillation frequency, essentially producing a continuous and simultaneous measurement of all defined OPRM cells.

(4) Trip Function

APRM System trips including OPRM trips are summarized in Table 7.6-2. The APRM scram trip function is discussed in Section 7.2. The APRM rod block trip function is discussed in Subsection 7.7.1.2. The APRM channels also provide trip signals indicating when an APRM channel is upscale, downscale, bypassed, or inoperative.

For the OPRM trip function, the response signal of any one OPRM cell that satisfies the conditions and criteria of the trip algorithm will cause a trip of the associated OPRM channel. Figure 7.6-14 illustrates the trip algorithm logic. The OPRM trip function does not have its own inoperative trip for insufficient number of total LPRM inputs in the channel. It follows the APRM's inoperative trip of insufficient number of LPRMs.

(5) Bypasses and Interlocks

(a) APRM

One APRM channel may be bypassed at any time. The trip logic will in essence become two-out-of-three instead of two-out-of-four.

The APRM also sends an interlock signal to the SSLC similar to the SRNM "ATWS Permissive" signal (Table 7.6-2). If this signal is a "high" level indicating the power is above the setpoint, this will allow the SSLC to permit ATWS protection action.

(b) OPRM

The OPRM channel bypass is controlled by the bypass of the APRM channel it resides with. Bypass of the APRM channel will bypass the OPRM trip function within this APRM channel. The OPRM also has its own separate automatic bypass functions: the OPRM trip output from any cell is bypassed if: (1) the APRM reading of the same channel is below 30% of rated power or the core flow reading is above 60% of rated flow; (2) the number of LPRM inputs to this OPRM cell is less than two. Any LPRM input to an OPRM cell is automatically bypassed if this LPRM reading is less than 5% of full scale LPRM reading. There is no requirement as to how many cells per OPRM channel has to be active since this is controlled by the total number of active LPRMs to the APRM channel.

(6) Redundancy

(a) APRM

There are four independent channels of the APRM monitor neutron flux, each channel being associated with one RPS division. Any two of the four APRM channels which indicate an abnormal condition will initiate a reactor scram via the RPS two-out-of-four logic. The redundancy criteria are met so that in the event of a single failure under permissible APRM bypass conditions, a scram signal can be generated in the RPS as required.

(b) OPRM

There are four independent and redundant OPRM channels. The above APRM redundancy condition also applies to OPRM since each OPRM is a subsystem of each of the four APRM channels. The OPRM trip outputs also follow the two-out-of-four logic as the APRM since the OPRM trip outputs are combined with other APRM trip outputs in each APRM channel to provide the final trip outputs to the RPS. In addition, each LPRM string with four LPRM detectors provides one LPRM input to each of the four independent and redundant OPRM channels. This provides core regional monitoring by redundant OPRM channels.

(7) Testability

APRM channels are calibrated using data from previous full-power runs and are tested by procedures in the instruction manual. Each APRM channel can be tested individually for the operability of the APRM scram and rod-blocking functions by introducing test signals. This includes the test for the OPRM trip function. A self-testing feature similar to that described for SSLC is also provided.

(8) Environmental Considerations

All APRM equipment is operated in the environments described in Section 3.11. The APRM is capable of functioning during and after the design basis events in which continued APRM operation is required (Sections 3.10 and 3.11).

#### 7.6.1.1.3 Reactor Operator Information

The man-machine interface of the Neutron Monitoring System provides for the information and controls described in this subsection. The lists provided in Table 7.6-3 consist of major signal information which is also documented in the system IED (Figure 7.6-1) and the system IBD (Figure 7.6-2).

### 7.6.1.2 Process Radiation Monitoring System—Instrumentation and Controls

A number of radiation monitoring functions are provided on process lines, HVAC ducts, and vents that may serve as discharge routes for radioactive materials. These include the following:

(1) Main steamline tunnel area

(2) Reactor Building ventilation exhaust (including fuel handling area)

(3) Control Building air intake supply

(4) Drywell sumps liquid discharge

(5) Radwaste liquid discharge

(6) Offgas discharge (pre-treated and post-treated)

(7) Gland steam condenser offgas discharge

(8) Plant stack discharge

(9) Turbine Building vent exhaust

(10) Standby gas treatment ventilation exhaust

(11) Radwaste Building ventilation exhaust

The process radiation subsystems are shown in the system design IED (Figure 7.6-5). Subsystems (1) through (4) are classified nuclear safety-related, while subsystems (5) through (11) are classified as non-safety-related. System descriptions and requirements are described in detail in Section 11.5.

### 7.6.1.3 High Pressure/Low Pressure Systems Interlock Protection Functions

(1) Function Identification

The low pressure modes of the RHR System which connect to the reactor coolant pressure boundary (RCPB) and the instrumentation which protects them from overpressurization are discussed in this section. Such high pressure/low pressure (HP/LP) interfaces with the reactor vessel are exclusive to the RHR System for the ABWR. The RHR P&ID is shown on Figure 5.4-10. The RHR IBD may be found on Figure 7.3-4.

(2) Power Sources

The power for the interlocks is provided from the essential power supplies used for the RHR System and its various modes of operation.

(3) Equipment Design

Refer to Table 7.6-3 for a list of HP/LP interfaces and the rationale for valve interlock equipment.

(4) Circuit Description

At least two valves are provided in series in each of these lines. The RHR shutdown cooling supply valves have independent sets of interlocks to prevent the valves from being opened when the primary system pressure is above the subsystem design pressure or when reactor water level is below Level 3. These valves also receive a signal to close when reactor pressure is above system pressure, or reactor water level is below Level 3. An additional interlock is RHR equipment area ambient temperature (not shown on Table 7.6-3).

The RHR shutdown cooling/LPFL injection valve is interlocked to prevent valve opening whenever the reactor pressure is above the subsystem design pressure, and automatically closes whenever the reactor pressure exceeds the subsystem design pressure. This valve must operate for long-term cooling, and has a remote testable check valve downstream. The check valve position can be confirmed at any time.

(5) Logic and Sequencing

The logic for the pressure and level sensor inputs is two-out-of-four high pressure or low level signals for valve closure. The additional RHR equipment area temperature signals for the shutdown suction valves consist of a single input channel for each valve.

(6) Bypasses and Interlocks

There are no additional bypasses or interlocks in the HP/LP interlocks themselves.

(7) Redundancy and Diversity

Each process line has two valves in series which are redundant in assuring the interlock. Each shutdown cooling supply and return valve has independent

and diverse interlocks to prevent the valves from being opened under the following conditions (Subsection 7.4.2.3.2 (4a)):

(a) Reactor pressure is above the RHR System design pressure.

(b) Reactor water level is below Level 3.

(c) RHR equipment area ambient temperature is above setpoint.

(8) Actuated Devices

The motor-operated valves are the actuated devices.

(9) Separation

Separation is maintained in the instrumentation portion of the HP/LP interlocks by assigning the signals for the electrically controlled valves to ESF separation divisions. The pressure and level sensors are supplied from the Nuclear Boiler System and are shared with other systems. There is one sensor from each of the four divisions, whose signal is passed through optical isolators and then the two-out-of-four voting logic (in combination with the signals from the other three divisions). The resultant signal is used to actuate each valve. Each division has its own isolation and two-out-of-four voting logic hardware (sheet 2 of RHR IBD, Figure 7.3-4).

(10) Testability

Since the HP/LP interlock valves are specifically designed to close under all conditions for normal reactor pressure, they cannot be tested during reactor operation. However, the sensors and logic can be tested during reactor operation in the same manner that the LPFL sensors and logic are tested. Refer to Subsection 7.3.1.1.1.4, 3(g) for a discussion of typical LPFL testing.

(11) Environmental Considerations

The instrumentation and controls for the HP/LP interlocks are qualified as Class 1E equipment. The sensors are mounted on local instrument panels and the control circuitry is housed in control panels in the control room.

(12) Operational Considerations

The HP/LP interlocks are strictly automatic. There is no manual bypass capability. If the operator initiates the RHR System, the interlocks will prevent RHR System exposure to high reactor pressure.

(13) Reactor Operator Information

The status of each valve providing the HP/LP boundary is indicated in the control room. The state of the sensors is also indicated in the control room.

(14) Setpoints

See Chapter 16 for setpoints and margin.

### 7.6.1.4 Not Used

### 7.6.1.5 Wetwell-to-Drywell Vacuum Breaker System—Instrumentation and Controls

This system is described in Chapter 6.

### 7.6.1.6 Containment Atmospheric Monitoring (CAM) System—Instrumentation and Controls

(1) System Identification

The CAM System (Figures 7.6-7 and 7.6-8) consists of two independent but redundant Class 1E divisions (I and II), which are electrically and physically separated. Each CAM division has the capability of monitoring the total gamma-ray dose rate and concentration of hydrogen and oxygen ($H_2/O_2$) in the drywell and/or the suppression chamber during plant operation, and following a LOCA event.

There are two radiation monitoring channels per division; one for monitoring the radiation level in the drywell and the other for monitoring the radiation level in the suppression chamber. Each monitoring channel consists of an ion chamber detector, a digital log radiation monitor, and a recorder. Each radiation monitoring channel provides alarm indication in the control room on high radiation levels and also if the channel becomes inoperative.

Each divisional $H_2/O_2$ monitoring channel consists of valves, pumps, and pipes used to extract samples of the atmosphere in the drywell or the suppression chamber and feed the extracted air sample into an analyzer and monitor for measurement, recording, and for alarm indication on high concentration of gas levels.

The piping used for the gas extraction is made of stainless steel and utilizes heat tracing to keep the pipes dry and free of moisture condensation.

(2) Power Sources

Each CAM Subsystem is powered from divisional 120 VAC instrument bus. The same Class 1E divisional 120 VAC power source also supplies the heat tracing blanket used for the sampling lines.

(3) Initiating Circuits

Each divisional gamma radiation monitoring channel can be energized manually by the operator or automatically by the LOCA signal. For the manual mode, the gamma radiation monitor is on continuously during plant operation and remains on until power is turned off by the operator.

In the power off mode, the channel will be activated automatically in the presence of a LOCA (high drywell pressure or low reactor water level).

Each divisional $H_2/O_2$ monitoring subsystem (except for the two sampling pumps) is powered continuously during plant operation. One pump is controlled by an operator and is used during reactor operation and the other is turned on by the LOCA signal to allow measurement during an accident.

The heat tracing used in each $H_2/O_2$ sample line is temperature controlled to prevent moisture condensation in the pipes.

Each divisional $H_2/O_2$ analyzer and monitor can selectively measure the atmosphere in the drywell or the suppression chamber.

Division I and II LOCA signals are provided to the CAM System from the RHR System. These signals are based on two-out-of-four logic signals for the high drywell pressure or low reactor water level.

(4) Redundancy and Diversity

The CAM Subsystems, Divisions I and II, are independent and are redundant to each other.

(5) Divisional Separation

The two CAM Subsystems are electrically and physically separated so that no single design basis event is capable of damaging equipment in more than one CAM division. No single failure or test, calibration, or maintenance operation can prevent function of more than one division.

(6) Testability and Calibration

Each CAM Subsystem can be tested separately during plant operation to determine the operational availability of the system. Each CAM Subsystem can be tested and calibrated separately.

Gas calibration sources are provided to check the hydrogen/oxygen sensors during normal plant operation and after an accident.

(7) Environmental Consideration

The CAM System is qualified Seismic Category I and is designed for operability during normal and post-accident environments.

(8) Operational Considerations

The following information is available to the reactor operator:

(a) Each gamma radiation channel consists of an ion chamber, a log radiation monitor, and a recorder. Each channel has a range of 0.01 Gy/h to $10^5$ Gy/h. Each channel will initiate an alarm on high radiation level or on an inoperative channel.

(b) Each hydrogen/oxygen monitoring channel uses a sampling rack for extracting the atmosphere from the drywell or the suppression chamber and for analyzing the contents for both $H_2/O_2$ concentration. The gaseous measurements are made by volume on a wet basis after humidity correction (dry basis before humidity correction). Separate monitors are provided for oxygen and hydrogen indications.

Each $H_2/O_2$ analyzer rack has a series of alarms to indicate a high concentration of hydrogen and of oxygen, and to alert the operator of any abnormal system parameter. Refer to Figure 7.6-8 for definition of these alarms.

(9) Control and Protective Functions

The CAM System does not provide control signals either to trip or to actuate other safety-related systems. However, the CAM System utilizes internal safeguards to affect system operation, alert the operator of abnormal performance, and protect equipment from damage.

### 7.6.1.7 Suppression Pool Temperature Monitoring System—Instrumentation and Controls

#### 7.6.1.7.1 System Identification

The Suppression Pool Temperature Monitoring (SPTM) System is provided to monitor suppression pool temperature. Monitoring of suppression pool temperature is provided so that trends in suppression pool temperature may be established in sufficient time for proper cooling of the suppression pool water and for reactor scram due to high suppression pool temperature and for reactor power control based upon symptom-based emergency operating procedures.

The SPTM System also provides information on the post-LOCA condition of the suppression pool.

The SPTM system IED is shown on Figure 7.6-11. Control system logic is shown on the IBD (Figure 7.6-12).

### 7.6.1.7.2 Power Sources

The instrumentation and controls of the SPTM System are powered by four divisionally separated 120 VAC buses (Divisions I, II, III and IV).

### 7.6.1.7.3 Equipment Design

The SPTM System configuration is shown in Figures 7.6-9 and 7.6-10. There are eight temperature circumferential sensor locations (Figure 7.6-9), which are chosen based upon the following considerations:

(1) To reliably measure the average bulk temperature of the suppression pool under normal plant operating conditions.

(2) Each SRV is in direct sight of two sets of temperature sensors within 9 meters.

(3) The sensors are not in direct paths of jet impingement such as horizontal vent flow and SRV quencher discharge.

(4) The sensors can be located without structural interference from the two equipment and personnel access tunnels.

Each temperature sensor location has a flexibility of ±5° in the azimuthal direction so that any interference with other equipment in the pool such as suction pipelines or undesirable locations such as proximity to a horizontal vent may be avoided.

At each temperature sensor location, there are two groups of sensors; one group for each of two divisions (Divisions I and III or Divisions II and IV) of sensors. Each group has four sensors located at different elevations in the suppression pool. At each sensor location, the two groups of sensors are to be separated by 15-30 cm in the azimuthal direction. The sensor envelope is given in Figure 7.6-9 and a cross section of a typical sensor location is given in Figure 7.6-10. The location of the temperature sensors are chosen based upon the following considerations:

(1) Sensors are located away from jet paths from horizontal vents and SRV discharge.

(2) Sensors are located at least 1m away from any wall or 160 mm structural member.

(3) Sufficient flexibility is allowed to facilitate sensor location and installation.

(4) Sensors are located to provide redundancy in measuring the average bulk suppression pool temperature.

(5) Sufficient sensors are located to measure the average bulk suppression pool temperature under accident conditions when the pool level drops to a level where complete condensation of vent flow and SRV discharge is still assured (i.e., 610 mm above the top of the first row of horizontal vents).

Electrical wiring for each sensor is terminated, for sensor replacement or maintenance, in the wetwell. This termination is sealed for moisture protection from condensation or wetwell sprays. Division I, II, III and IV sensors are wired through Division I, II, III or IV electrical penetrations, respectively. Division I, II, III or IV sensor signals are wired to the Remote Shutdown System all sensor signals multiplexed to the main control room via the respective Division I, II, III or IV essential multiplexers.

#### 7.6.1.7.4 Signal Conditioning

The suppression pool temperatures within a division are average to determine a mean temperature of the pool. The average is corrected for failed sensors. Sensors exposed to air temperature are also excluded.

#### 7.6.1.7.5 Trip Function

The SPTM system provides trip signals for each of the four divisions (for two-out-of-four logic) indicating when the suppression pool temperature has exceeded the high limit.

#### 7.6.1.7.6 Bypasses and Interlocks

The SPTM System has no bypasses and interlocks. A division of sensors can be bypassed to allow maintenance.

#### 7.6.1.7.7 Control Action

The SPTM System initiates RHR suppression pool cooling, RCW load shedding and RPS scram signaling. It also provides measurement, indication, and recording, and initiates alarms in the main control room and in the remote shutdown panel.

#### 7.6.1.7.8 Divisional Separation

The four SPTM System divisions are electrically separated so that no single design basis event is capable of damaging equipment in more than one division. No single failure or test, calibration, or maintenance operation can prevent function of more than one division.

#### 7.6.1.7.9 Signal Processing

Processing of temperature signals is performed by a microprocessor for each instrument division. For each of the four instrument divisions, the temperature signals are arithmetically averaged to yield an average bulk suppression pool temperature. Provisions are incorporated to detect sensor failures. When failure of a sensor is detected, its output is not added to the sum of all other sensors in the division and the number of sensors is correspondingly reduced in computing the average temperature. In addition, the narrow range suppression pool water level signal from the Atmospheric Control System (ACS) is used to detect uncovery of the first set of sensors below the pool surface. After sensor installation, the elevation for each sensor is to be established with respect to a common reference elevation. When the suppression pool water level drops below the elevation of a particular sensor, that sensor signal is not used in computing the average. The wide range level signal from the ACS is utilized for this purpose for the remaining sensors.

#### 7.6.1.7.10 Output Signals

For each division of the SPTM System, each temperature sensor output and the average bulk suppression pool temperature can be individually addressable for display. These signals can also be selectable and provided for continuous recording. The recording device need not be a Class 1E device.

For each SPTM division, high bulk average temperature is annunciated. Four sensors from Division I and four sensors from Division II are sent to the remote shutdown panel.

In addition to the system display recording, and alarm functions, outputs from the SPTM System to other systems are provided as shown in Table 7.6-4.

When signals are provided from the SPTM System to other systems, signal isolation is provided between one instrument division to another division. For example, the Division I suppression pool high bulk average temperature signal to Division II and III of the RHR System is optically isolated via its fiber-optic interface medium.

#### 7.6.1.7.11 Testability and Calibration

Each SPTM System division is testable during plant operation to determine the operational availability of the system. Each SPTM division has the capability for test, calibration, and adjustments.

#### 7.6.1.7.12 Environmental Consideration

The SPTM System local equipment is designed to be continuously operable during normal and post-accident environments. Indicating and recording equipment located in the main control room is designed to operate in the environment of the control room.

## 7.6.2 Analysis

### 7.6.2.1 Neutron Monitoring System—Instrumentation and Controls

The analysis for the trip inputs from the Neutron Monitoring System (NMS) to the Reactor Protection (trip) System are discussed in Subsection 7.2.2.

The automatic traversing in-core probe (ATIP) is a non safety-related subsystem of the NMS and is analyzed along with the other non safety subsystems in Subsection 7.7.2.

This analysis section covers only the safety-related subsystems of the NMS. These include the following:

(1) Startup Range Neutron Monitor Subsystem (SRNM)

(2) Power Range Neutron Monitor Subsystem (PRNM) which includes:

(a) Local Power Range Monitor Subsystem (LPRM)

(b) Average Power Range Monitor Subsystem (APRM)

#### 7.6.2.1.1 General Functional Requirements Conformance

(1) Startup Range Neutron Monitors (SRNM)

The SRNM Subsystem is designed as a safety-related system that will generate a scram trip signal to prevent fuel damage in the event of any abnormal reactivity insertion transients while operating in the startup power range. This trip signal is generated by either an excessively high neutron flux level, or too fast a neutron flux increase rate (i.e., reactor period). The setpoints of these trips are such that under worst reactivity insertion transients, fuel integrity is always protected. The independence and redundancy requirements are incorporated into the design of the SRNM and are consistent with the safety design bases of the Reactor Protection System (RPS).

(2) Power Range Neutron Monitors (PRNM)

The PRNM Subsystem provides information for monitoring the average power level of the reactor core and for monitoring the local power level when the reactor power is in the power range (above approximately 15% power). It mainly consists of the LPRM and the APRM Subsystems.

(a) LPRM Subsystem: The LPRM is designed to provide a sufficient number of LPRM signals to the APRM System such that the safety design basis for the APRM is satisfied. The LPRM itself has no safety design basis. However, it is qualified as a safety-related system.

(b) APRM Subsystem: The APRM is capable of generating a trip signal to scram the reactor in response to excessive and unacceptable neutron flux increase, in time to prevent fuel damage. Such a trip signal also includes a trip from the simulated thermal power signal which is a properly delayed signal from the APRM signal. It also includes a trip from a core flow based algorithm which will issue a trip if the core flow suddenly decreases too fast, called the Core Flow Rapid Coastdown trip. It also includes a trip from the OPRM subsystem algorithm which will issue a trip if the OPRM algorithm detects a growing neutron flux oscillation indicating core thermal hydraulic instability. All scram functions are assured so long as the minimum LPRM input requirement to the APRM is satisfied. If such an input requirement cannot be met, a trip signal shall also be generated. The independence and redundancy requirements are incorporated into the design and are consistent with the safety design basis of the RPS.

#### 7.6.2.1.2 Specific Regulatory Requirements Conformance

Table 7.1-2 identifies the Neutron Monitoring System (NMS) 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-279)

The safety-related subsystems of the neutron monitoring system consist of four divisions which correspond and interface with those of the RPS. This independence and redundancy assure that no single failure will interfere with the system operation.

The 10 SRNM channels are divided into four divisions and independently assigned to three bypass groups such that up to three SRNM channels are allowed to be bypassed at any time while still providing the required monitoring and protection capability.

There are 52 LPRM assemblies evenly distributed in the core. There are four LPRM detectors on each assembly, evenly distributed from near the bottom of the fuel region to near the top of the fuel region (Figure 7.6-3). A total of 208 detectors are divided and assigned to four divisions for the four APRMs. Any single LPRM detector is only assigned to one APRM division. Electrical wiring and physical separation of the division is optimized to satisfy the safety-related system requirement. With the four divisions, redundancy criteria are met, since a scram signal can still be initiated with a postulated single failure under

allowed APRM bypass conditions. The OPRM subsystem as described in Subsection 7.6.1.1.2.2 conforms to all applicable requirements of IEEE-279.

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

All applicable requirements of IEEE-279 are met with the NMS.

(2) General Design Criteria (GDC)

In accordance with the Standard Review Plan for Section 7.6, and with Table 7.1-2, the following GDCs are addressed for the NMS:

(a) **Criteria**—GDCs 2, 4, 10, 12, 13, 19, and 28.

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

(3) Regulatory Guides (RGs)

In accordance with the Standard Review Plan for Section 7.6, and with Table 7.1-2, the following RGs are addressed for the NMS:

(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 1.75— "Physical Independence of Electric Systems"

(e) RG 1.97— "Instrumentation During and Following an Accident"

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

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

The NMS conforms with all the above-listed RGs, assuming the same interpretations and clarifications identified in Subsections 7.2.2.2.1(7), 7.3.2.1.2 and 7.1.2.10.

* See Subsection 7.1.2.10.9.

(4) Branch Technical Positions (BTPs)

In accordance with the Standard Review Plan for Section 7.6, and with Table 7.1-2, only BTPs 21 and 22 are considered applicable for the NMS. 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 NMS is in full compliance with this BTP.

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

The NMS is continuously operating during reactor operation. The accuracy of the sensors can be verified by cross-comparison of the various channels within the four redundant divisions. The bypass of any RPS division will cause the two-out-of-four trip voting logic to revert to two-out-of-three. Therefore, the NMS fully meets this BTP.

(5) TMI Action Plan Requirements (TMI)

In accordance with the Standard Review Plan for Section 7.6, and with Table 7.1-2, there are no TMI action plan requirements applicable to the NMS. However, all TMI requirements are addressed in Appendix 1A.

### 7.6.2.2 Process Radiation Monitoring System—Instrumentation and Controls

This analysis section covers only the safety-related subsystems of the Process Radiation Monitoring (PRM) System as identified in Subsection 7.6.1.2.

#### 7.6.2.2.1 General Functional Requirements Conformance

The Process Radiation Monitoring (PRM) System samples and/or monitors the radioactivity levels in process and effluent streams, initiates protective actions to prevent further release of radioactive material to the environment, and activates alarms in the control room to alert operating personnel to the high radiation activity.

#### 7.6.2.2.2 Specific Regulatory Requirements Conformance

Table 7.1-2 identifies the PRM 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-279):

Each safety-related PRM subsystem, except for the drywell sump discharge radiation monitor, utilizes four redundant divisional channels in a two-out-of-four voting logic to initiate the protective action. This redundancy satisfies the single-failure criterion such that a failure of a single element will not interfere with the system to perform its intended safety function. The drywell sump discharge radiation monitor consists of one channel per drywell sump, and is used to terminate the transfer of the liquid waste to the Radwaste Building when the high radiation level is detected in the discharged liquid waste. Failure of this channel to isolate the drain line is not considered detrimental to plant safety or operation. Failure of the radiation channel will be indicated by the monitor and the operator will be alerted in time to take corrective action.

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

Electrical separation is maintained between the redundant divisions. All applicable requirements of IEEE-279 are met by the safety-related subsystem of the PRM System.

(2) General Design Criteria (GDC)

In accordance with the Standard Review Plan for Section 7.6, and with Table 7.1-2, the following GDCs are addressed for the PRM:

(a) **Criteria—**GDCs 2, 4, 13, 16, 19, 20, 21, 22, 23, 24, and 28.

(b) **Conformance—**The safety-related PRM subsystems are in compliance with these GDCs, in part, or as a whole, as applicable. The GDCs are generically addressed in Subsection 3.1.2.

(3) Regulatory Guides (RGs)

In accordance with the Standard Review Plan for Section 7.6, and with Table 7.1-2, the following RGs are addressed for the PRM safety-related subsystems:

(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 PRM safety-related subsystems 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. A generic assessment of RG 1.97 is provided in Section 7.5.

(4) Branch Technical Positions (BTPs)

In accordance with the Standard Review Plan for Section 7.6, and with Table 7.1-2, only BTPs 21 and 22 are considered applicable for the PRM safety-related subsystems. 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 PRM System is in full compliance with this BTP.

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

The PRM monitors are continuously operating and are self-tested during reactor operation. Self-test is continuous and detected faults are indicated and/or annunciated.

(5) TMI Action Plan Requirements (TMI)

In accordance with the Standard Review Plan for Section 7.6, and with Table 7.1-2, only TMI II.F.3— "Instrumentation for Monitoring Accident Conditions" is considered applicable for the PRM System.

This and all other TMI action plan requirements are addressed in Appendix 1A. A generic assessment of Regulatory Guide 1.97 is presented in Section 7.5.

### 7.6.2.3 High Pressure/Low Pressure Systems Interlock Function

The ABWR has only one low pressure system, the RHR System, which interfaces with the reactor pressure boundary and requires HP/LP interlock protection. However, the RHR System has several modes of operation which are addressed in other Tier 2 sections.

#### 7.6.2.3.1 General Functional Requirements Conformance

The HP/LP interlocks provide an interface between the low pressure RHR System and reactor pressure. When reactor pressure is low enough to not be harmful to the low pressure system, the valves open and expose the low pressure system to reactor pressure. The interlocks are automatic and the operator is given indication of their status.

Each HP/LP interface consists of two valves in series; one inside and one outside the drywell wall. The injection lines are used for both the Low Pressure Flooder mode (LPFL), and the Shutdown Cooling (SDC) mode. The isolation valves on these lines consist of a motor-operated valve (MOV) in series with a check valve. The suction lines have MOVs on both inboard and outboard sides.

Redundancy is integrated into the design by placing the inboard and outboard shutdown cooling suction valves on different electrical power divisions for each RHR loop. A diversity of signals (high reactor pressure or low reactor water level) is used to actuate closure of the two motor-operated suction valves. This is further described in 4(a) of Subsection 7.4.2.3.2.

#### 7.6.2.3.2 Specific Regulatory Requirements Conformance

Table 7.1-2 identifies the HP/LP interlocks 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-279)

The HP/LP interlocks are an integral part of the RHR System, which is designed to meet the requirements of IEEE-279 as discussed in Subsections 7.4.2.3.2 and 7.3.2.1.2.

(2) General Design Criteria (GDC)

In accordance with the Standard Review Plan for Section 7.6, and with Table 7.1-2, the following GDCs are addressed for the HP/LP interlocks:

(a) **Criteria—**GDCs 2, 4, 10, 13, 15, 19, 33, and 44.

(b) **Conformance—**The HP/LP interlocks are in compliance with these GDCs, in part, or as a whole, as applicable. The GDCs are generically addressed in Subsection 3.1.2.

(3) Regulatory Guides (RGs)

In accordance with the Standard Review Plan for Section 7.6, and with Table 7.1-2, the following RGs are addressed for the HP/LP interlocks:

(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 HP/LP interlocks are designed to assure that the HP/LP isolation valves close when reactor pressure exceeds the design pressure for the low pressure RHR System. Since this function is deliberately designed so that it cannot be bypassed, it is not possible to test these interlocks nor the associated valves during the higher pressure conditions of the normally operating reactor. However, they can be routinely tested when the reactor is shut down.

Otherwise, the interlocks are designed to meet the same requirements as the RHR System, as addressed in Subsections 7.3.2.1.2 and 7.4.2.3.2.

(4) Branch Technical Positions (BTPs):

In accordance with the Standard Review Plan for Section 7.6, and with Table 7.1-2, the following BTPs are considered applicable to the HP/LP interlocks:

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

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

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

These BTPs are addressed with respect to the HP/LP interlocks in Subsection 7.4.2.3.2 (4).

(5) TMI Action Plan Requirements (TMI):

In accordance with the Standard Review Plan for Section 7.6, and with Table 7.1-2, there are no TMI action plan requirements applicable to the HP/LP interlocks. However, all TMI requirements are addressed in Appendix 1A.

### 7.6.2.4 Not Used

### 7.6.2.5 Wetwell-to-Drywell Vacuum Breaker System—Instrumentation and Controls

This system is passive and has no electrical interface. It is described in Subsection 6.2.1.1.4.1.

### 7.6.2.6 Containment Atmospheric Monitoring System—Instrumentation and Controls

#### 7.6.2.6.1 General Functional Requirements Conformance

The Containment Atmospheric Monitoring System (CAMS) provides normal plant operation and post-accident monitoring for gross gamma radiation and hydrogen/oxygen concentration levels in both the drywell and suppression chamber. Main control room display and annunciation indicate the gamma and hydrogen/oxygen levels to the plant personnel.

#### 7.6.2.6.2 Specific Regulatory Requirements Conformance

Table 7.1-2 identifies the CAMS 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-279)

The CAMS consists of two divisions which are redundantly designed so that failure of any single element will not interfere with the system operation. Electrical separation is maintained between the redundant divisions.

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 system can be actuated manually by the operator, or it is automatically initiated by a LOCA signal (high drywell pressure or low reactor water level).

The CAMS does not actuate nor interface with the actuation of any other safety-related system. Therefore, any portion of IEEE-279 which pertains to such interfaces is not applicable. All other applicable requirements of IEEE-279 are met with the CAMS.

(2) General Design Criteria (GDC)

In accordance with the Standard Review Plan for Section 7.6, and with Table 7.1-2, the following GDCs are addressed for the CAMS:

(a) **Criteria—**GDCs 2, 4, 13, 16, 19, and 41.

(b) **Conformance—**With regard to GDC 41, the CAMS is not designed to control or clean up the containment atmosphere. It merely monitors such, and indicates levels and initiates alarms on high levels. The Standby Gas Treatment System (SGTS) controls fission products sufficient for the inerted containment (Subsections 7.3.1.1.5 and 7.3.2.5).

Conformance with the above listed GDCs is met as a whole, or in part, as applicable. All GDCs are generically addressed in Subsection 3.1.2.

(3) Regulatory Guides (RGs)

In accordance with the Standard Review Plan for Section 7.6, and with Table 7.1-2, the following RGs are addressed for the CAMS:

(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 1.75— "Physical Independence of Electric Systems"

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

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

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

Regulatory Guide 1.22 is not applicable to the CAMS because the CAMS does not actuate or provide controls to any protective system. The CAMS

* See Subsection 7.1.2.10.9.

is in conformance with all other RGs listed, assuming the same interpretations and clarifications identified in Subsections 7.3.2.1.2 and 7.1.2.10. A generic assessment of RG 1.97 is provided in Section 7.5.

(4) Branch Technical Positions (BTPs)

In accordance with the Standard Review Plan for Section 7.6, and with Table 7.1-2, only BTPs 21 and 22 are addressed for the CAMS 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 CAMS is in full compliance with this BTP.

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

CAMS performs no actuation functions. Therefore, this BTP is not applicable to the CAMS.

(5) TMI Action Plan Requirements (TMI)

In accordance with the Standard Review Plan for Section 7.6, and with Table 7.1-2, the following TMI action plan requirements are addressed for the CAMS:

(a) TMI II.F.1— "Accident Monitoring Instrumentation Positions"

(b) TMI II.F.3— "Monitoring Accident Conditions (RG 1.97)"

The CAMS provides safety-related instrumentation for use during and after LOCA events and is in compliance with RG 1.97. These TMIs are addressed generically in Appendix 1A. An assessment of RG 1.97 is presented in Section 7.5.

### 7.6.2.7 Suppression Pool Temperature Monitoring System—Instrumentation and Controls

#### 7.6.2.7.1 General Functional Requirements Conformance

Instrumentation is provided for automatic reactor scram or automatic suppression pool cooling initiation. Visual indications for operator awareness of pool temperature under all operating and accident conditions is also provided. The system is automatically initiated and continuously monitors pool temperatures during reactor operation.

#### 7.6.2.7.2 Specific Regulatory Requirements Conformance

Table 7.1-2 identifies the SPTM 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-279)

The SPTM System consists of four divisions which are redundantly designed so that failure of any single element will not interfere with the system operation. There are four levels of temperature monitoring within each division. Electrical separation is maintained between the redundant divisions.

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 SPTM system continuously operates during plant operation. It does, however, automatically initiate RHR for suppression pool cooling, initiates RCW for load shedding to increase suppression pool cooling and generates four divisional trip signals for RPS. Therefore, the portions of IEEE 279 which pertain to actuation of safety functions apply through RHR and RPS. All other applicable requirements of IEEE 279 are met with the SPTM system.

(2) General Design Criteria (GDC)

In accordance with the Standard Review Plan for Section 7.6 and with Table 7.1-2, the following GDCs are addressed for the SPTM System:

(a) **Criteria**—GDCs 2, 4, 13, 16, 19, 20, 21, 22, 23, 24, 29 and 38.

(b) **Conformance**—With regard to GDC 20, 21, 22, 23, 24 and 29, the SPTM System generates four division trip signals for RPS and RPS generates the scram signal for the reactor trip.

With regard to GDC 38, the SPTM is not designed to control or remove heat from the containment. It monitors the suppression pool temperatures, generates operator displays, initiates alarms, and automatically initiates the suppression pool cooling mode of RHR. The SPC mode of the RHR System is sufficient to remove heat from the suppression pool (Subsections 7.3.1.1.4 and 7.3.2.4).

Conformance with the above listed GDCs is met as a whole, or in part, as applicable. All GDCs are generically addressed in Subsection 3.1.2.

(3) Regulatory Guides (RGs)

In accordance with the Standard Review Plan for Section 7.6, and with Table 7.1-2, the following RGs are addressed for the SPTM 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 1.75— "Physical Independence of Electric Systems"

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

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

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

The SPTM System is in conformance with all RGs listed, assuming the same interpretations and clarifications identified in Subsections 7.3.2.1.2 and 7.1.2.10. For RG 1.22, actuation is through RPS as stated in Subsection 7.6.2.7.2(1). A generic assessment of RG 1.97 is provided in Section 7.5.

(4) Branch Technical Positions (BTPs)

In accordance with the Standard Review Plan for Section 7.6, and with Table 7.1-2, only BTPs 21 and 22 need be addressed for the SPTM System. They are 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 SPTM System is in full compliance with this BTP.

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

As indicated in Subsection 7.6.2.7.2(1), the SPTM System performs no actuation functions; actuation is through RPS.

(5) TMI Action Plan Requirements (TMI)

In accordance with the Standard Review Plan for Section 7.6, and with Table 7.1-2, the following TMI action plan requirements are addressed for the SPTM System:

(a) TMI II.F.1— "Accident Monitoring Instrumentation Positions"

(b) TMI II.F.3— "Monitoring Accident Conditions (RG 1.97)"

The SPTM System provides safety-related instrumentation for use during and after LOCA events. However, these TMIs are addressed generically in Appendix 1A. An assessment of RG 1.97 is presented in Section 7.5.

## 7.6.3 COL License Information

### 7.6.3.1 APRM Oscillation Monitoring Logic

The COL applicant will implement the APRM oscillation monitoring logic function in accordance with the BWR Owner's Group as described in Subsection 7.6.1.1.2.2.

## Table 7.6-1 SRNM Trip Function Summary

| Trip Function | Trip Setpoint (Nominal) | Action |
|---|---|---|
| SRNM Upscale Flux Trip | 45% power* | Scram (bypassed in RUN) |
| SRNM Upscale Flux Alarm | 35% power† | Rod Block (bypassed in RUN) |
| SRNM Short Period Trip | 11 seconds | Scram‡ (bypassed in RUN & REFUEL) (no scram function in counting range) |
| SRNM Short Period Alarm | 21 seconds | Rod Block (bypassed in RUN) |
| SRNM Period Withdrawal Permissive | 56 seconds | Warning*f* (bypassed in RVN) |
| SRNM Inop | Module interlock disconnect HV voltage low Electronics Criteria Failure | Scram & Rod Block (bypassed in RUN) |
| SRNM Downscale | 3 cps | Rod Block |
| SRNM ATWS Permissive | 6% | All Modes** |
| SRNM Noncoincidence Upscale Flux Trip | 5E+5 cps | Scram (activated by manual switch in RPS)*f* |
| SRNM Noncoincidence Upscale Flux Alarm | 1E + 5 cps | Rod Block (activated by manual switch in RPS) |

* This scram setpoint is functionally equivalent to the upscale scram on the last range of BWR/5 IRM, at the 120/125 level.

† This rod block setpoint is functionally equivalent to the upscale rod block on the last range of BWR/5 IRM, at the 108/125 level.

‡ Scram action only active in MSV range, which is defined as above $1 \times 10^{-4}$% power.

*f* Conditions for activation will be defined in the technical specifications.

** All SRNM channels within each division have to indicate a power level below the setpoint in order to remove the permissive.

## Table 7.6-2 APRM Trip Function Summary

| Trip Function | Trip Setpoint (Nominal) | Action |
|---|---|---|
| **(a) APRM Trip Function** | | |
| APRM Upscale Flux Trip | 118% power<br>13% power | Scram (only in RUN)<br>Scram (not in RUN) |
| APRM Upscale Flux Alarm | Flow biased<br>10% power | Rod Block (only in RUN)<br>Rod Block (not in RUN) |
| APRM Upscale Thermal Trip | Flow biased | Scram |
| APRM Inoperative | 1. LPRM input too few<br>2. Module interlocks disconnect<br>3. Electronics Critical Failure | Scram & Rod Block |
| APRM Downscale | 5% Decrease* | Rod Block (only in RUN) |
| APRM ATWS Permissive | 6% | All Modes† |
| Core Flow Rapid Coastdown* | fixed* | Scram (bypassed with thermal power < 77%) |
| Core Flow Upscale Alarm | 120% (flow) | Rod Block (only in RUN) |
| **(b) OPRM Trip Function** | | |
| Growth Rate-Based Trip ($S_3$) | $S=S_3=(P_1-1.0) \times DR_3+1.0$‡<br>$DR_3=1.3$ | Scram*f* |
| Amplitude-Based Maximum Trip ($S_{max}$) | $S=S_{max}=1.30$‡ | Scram*f* |
| Period-Based Trip ($S_P$) | $S=S_P=1.10$** | Scram*f* |

* The trip signal is based on a flow-dependent equation. If the flow decreases too fast, the trip signal will reach the fixed trip setpoint and initiate scram. The thermal power signal is only used as a criteria to determine scram bypass condition.

† APRM has to indicate a power level below the setpoint in order to remove the permissive.

‡ $P_1$ is the last peak reading measured after the signal S exceeds $S_1$. Other Pre-Trip condition parameters of the algorithm are:

$S_1$=1.10, $S_2$=0.92, $T_1$=0.31 to 2.2 s, $T_2$=0.31 to 2.2 s.
(For details see Figure 7.6-14).

*f* Automatically bypassed if core power ≤30% or core flow ≥60%

** Other Pre-Trip Condition parameters of the algorithm are:

$T_{min}$=1 s, $T_{max}$=3.5 s, $\pm t_{error}$=0.15 s $N_P$=10.
(For details see Figure 7.6-14).

## Table 7.6-3 High Pressure/Low Pressure System Interlock Interfaces

| Interlocked Process Line | Type | Valve | Parameter Sensed | Purpose |
|---|---|---|---|---|
| RHR Shutdown Cooling Supply | MO<br>MO | E11-F010<br>E11-F011 | Reactor pressure, low level | Prevents valve opening until reactor pressure is low and level is above Level 3.* |
| RHR Shutdown Cooling/LPFL Injection | Check<br>MO | E11-F006<br>E11-F005 | N/A<br>Reactor pressure | N/A<br>Prevents valve opening until reactor pressure is low.† |

* Recloses valve if pressure is high, or level drops below Level 3.

† Recloses valve if pressure is high.

## Table 7.6-4 Outputs From SPTM System to Other Systems

| Signal | Utilization |
|---|---|
| 1. Division I suppression pool bulk average high temperature signal to RHR Divisions I, II & III | 1. Alarm and initiation of RHR suppression pool cooling |
| 2. Division II suppression pool bulk average high temperature signal to RHR Divisions I, II & III | 2. Alarm and initiation of RHR suppression pool cooling |
| 3. Division III suppression pool bulk average high temperature signal to RHR Divisions I, II & III | 3. Alarm and initiation of RHR suppression pool cooling |
| 4. Division IV suppression pool bulk average high temperature signal to RHR Divisions I, II & III | 4. Alarm and initiation of RHR suppression pool cooling |
| 5. Isolated composite Divisions I, II, III and IV suppression pool bulk average mean temperature signal to RCW | 5. Initiation of RCW for load shedding to increase suppression pool cooling |
| 6. Division I suppression pool bulk average high temperature trip signal to RPS Division I | 6. Alarm and RPS trip signal |
| 7. Division II suppression pool bulk average high temperature trip signal to RPS Division II | 7. Alarm and RPS trip signal |
| 8. Division III suppression pool bulk average high temperature trip signal to RPS Division III | 8. Alarm and RPS trip signal |
| 9. Division IV suppression pool bulk average high temperature trip signal to RPS Division IV | 9. Alarm and RPS trip signal |

## Table 7.6-5 Reactor Operator Information for NMS

(1) The NMS provides for the activations of the following annunciations at the main control panel:
- (a) SRNM neutron flux upscale reactor trip
- (b) SRNM neutron flux upscale rod block
- (c) SRNM neutron flux downscale rod block
- (d) SRNM short period reactor trip
- (e) SRNM short period rod block
- (f) SRNM inoperative reactor trip
- (g) SRNM period withdrawal permissive alarm
- (h) APRM neutron flux upscale reactor trip
- (i) APRM simulated thermal power reactor trip
- (j) APRM neutron flux upscale rod block
- (k) APRM neutron flux downscale rod block
- (l) Reference APRM downscale rod block
- (m) APRM system inoperative reactor trip
- (n) Core flow rapid coastdown reactor trip
- (o) APRM core flow upscale rod block
- (p) Core flow inoperative alarm
- (q) LPRM neutron flux upscale alarm
- (r) LPRM neutron flux downscale alarm
- (s) ATIP automatic control system (ACS) inoperative
- (t) ATIP indexer inoperative
- (u) ATIP control function inoperative
- (v) ATIP valve control monitor function inoperative
- (w) MRBM upscale rod block
- (x) MRBM downscale rod block
- (y) MRBM inoperative rod block
- (z) Core flow abnormal
- (aa) OPRM trip

(2) The NMS provides status information on the dedicated NMS operator interface on the main control panel as follows:
- (a) APRM power level
- (b) SRNM power level

(3) The dedicated operator interface of the NMS provides logic and operator controls, so that the operator can perform the following functions at the main control panel:
- (a) APRM channel bypass
- (b) SRNM channel bypass
- (c) MRBM main channel bypass

Acronyms

| | | |
|---|---|---|
| NMS | - | Neutron Monitoring System |
| SRNM | - | Startup Range Neutron Monitor |
| APRM | - | Average Power Range Monitor |
| LPRM | - | Local Power Range Monitor |
| ATIP | - | Automatic Traversing In-Core Probe |
| MRBM | - | Multi-channel Rod Block Monitor |
| CRT | - | Cathode Ray Tube |
| OPRM | - | Oscillation Power Range Monitor |

## Table 7.6-5 Reactor Operator Information for NMS (Continued)

(3) (Continued)
- (d) MRBM rod block logic test
- (e) MRBM upscale rod block setpoint setup to intermediate/normal

(4) Certain NMS-related information, available on the main control panel, is implemented in software which is independent of the process computer. This information is listed below.
- (a) SRNM reactor period
- (b) SRNM count rate
- (c) APRM bypass status
- (d) APRM neutron flux upscale trip/inoperative status
- (e) APRM neutron flux upscale rod block status
- (f) APRM neutron flux downscale rod block status
- (g) APRM core flow upscale rod block status
- (h) APRM core flow rapid coastdown status
- (i) APRM core flow rapid coastdown bypass status
- (j) MRBM main channel bypass status
- (k) MRBM main channel upscale rod block status
- (l) MRBM main channel downscale rod block status
- (m) MRBM main channel inoperative rod block status
- (n) MRBM main channel core flow abnormal rod block status
- (o) OPRM trip status

(5) CRT displays, which are part of the performance monitoring and control system, provide certain NMS-related displays and controls on the main control panel which are listed below:
- (a) SRNM upscale trip/inoperative status
- (b) SRNM reactor period trip status
- (c) SRNM upscale rod block status
- (d) SRNM reactor period rod block status
- (e) SRNM downscale rod block status
- (f) SRNM bypass status
- (g) SRNM period historical record
- (h) SRNM count rate historical record
- (i) SRNM period-based permissive
- (j) LPRM string selected for status readings
- (k) LPRM neutron flux level (designated group of LPRMs displayed upon selection of certain single rod or gang of control rods)
- (l) LPRM bypass status
- (m) LPRM neutron flux downscale alarm status
- (n) LPRM neutron flux upscale alarm status
- (o) Number bypassed LPRMs and APRM channel

Acronyms

| | | |
|---|---|---|
| NMS | - | Neutron Monitoring System |
| SRNM | - | Startup Range Neutron Monitor |
| APRM | - | Average Power Range Monitor |
| LPRM | - | Local Power Range Monitor |
| ATIP | - | Automatic Traversing In-Core Probe |
| MRBM | - | Multi-channel Rod Block Monitor |
| CRT | - | Cathode Ray Tube |
| OPRM | - | Oscillation Power Range Monitor |

## Table 7.6-5 Reactor Operator Information for NMS (Continued)

(5) (Continued)
- (p) APRM simulated thermal power reactor trip status
- (q) APRM core flow
- (r) Core flow historical record
- (s) APRM neutron flux
- (t) APRM simulated thermal power trip setpoint
- (u) APRM simulated thermal power
- (v) APRM simulated thermal power record
- (w) Reference APRM downscale rod block status (One for each MRBM main channel)
- (x) MRBM main channel block level status
- (y) MRBM main channel upscale (normal) rod block setpoint
- (z) MRBM main channel upscale (intermediate) rod block setpoint
- (aa) MRBM main channel upscale (low) rod block setpoint
- (ab) MRBM main channel upscale (normal) rod block setpoint historical record
- (ac) MRBM main channel upscale (intermediate) rod block setpoint historical record
- (ad) MRBM main channel upscale (low) rod block setpoint historical record
- (ae) MRBM subchannel inoperative status
- (af) MRBM subchannel upscale rod block status
- (ag) MRBM subchannel downscale rod block status
- (ah) MRBM subchannel intermediate level transfer rate
- (ai) MRBM subchannel normal level transfer rate
- (aj) MRBM subchannel reading
- (ak) MRBM subchannel reading historical record
- (al) MRBM subchannel setup permissive
- (am) MRBM gain adjustment failed
- (an) No rod selected (MRBM)
- (ao) Peripheral rod selected (MRBM)
- (ap) OPRM trip setpoint data
- (aq) OPRM cell configuration and status of LPRM inputs
- (ar) OPRM trip status
- (as) OPRM signals record

Acronyms

| | | |
|---|---|---|
| NMS | - | Neutron Monitoring System |
| SRNM | - | Startup Range Neutron Monitor |
| APRM | - | Average Power Range Monitor |
| LPRM | - | Local Power Range Monitor |
| ATIP | - | Automatic Traversing In-Core Probe |
| MRBM | - | Multi-channel Rod Block Monitor |
| CRT | - | Cathode Ray Tube |
| OPRM | - | Oscillation Power Range Monitor |

**The following figures are located in Chapter 21:**

**Figure 7.6-1 Neutron Monitoring System IED (Sheets 1-4)**

**Figure 7.6-2 Neutron Monitoring System IBD (Sheets 1-28)**

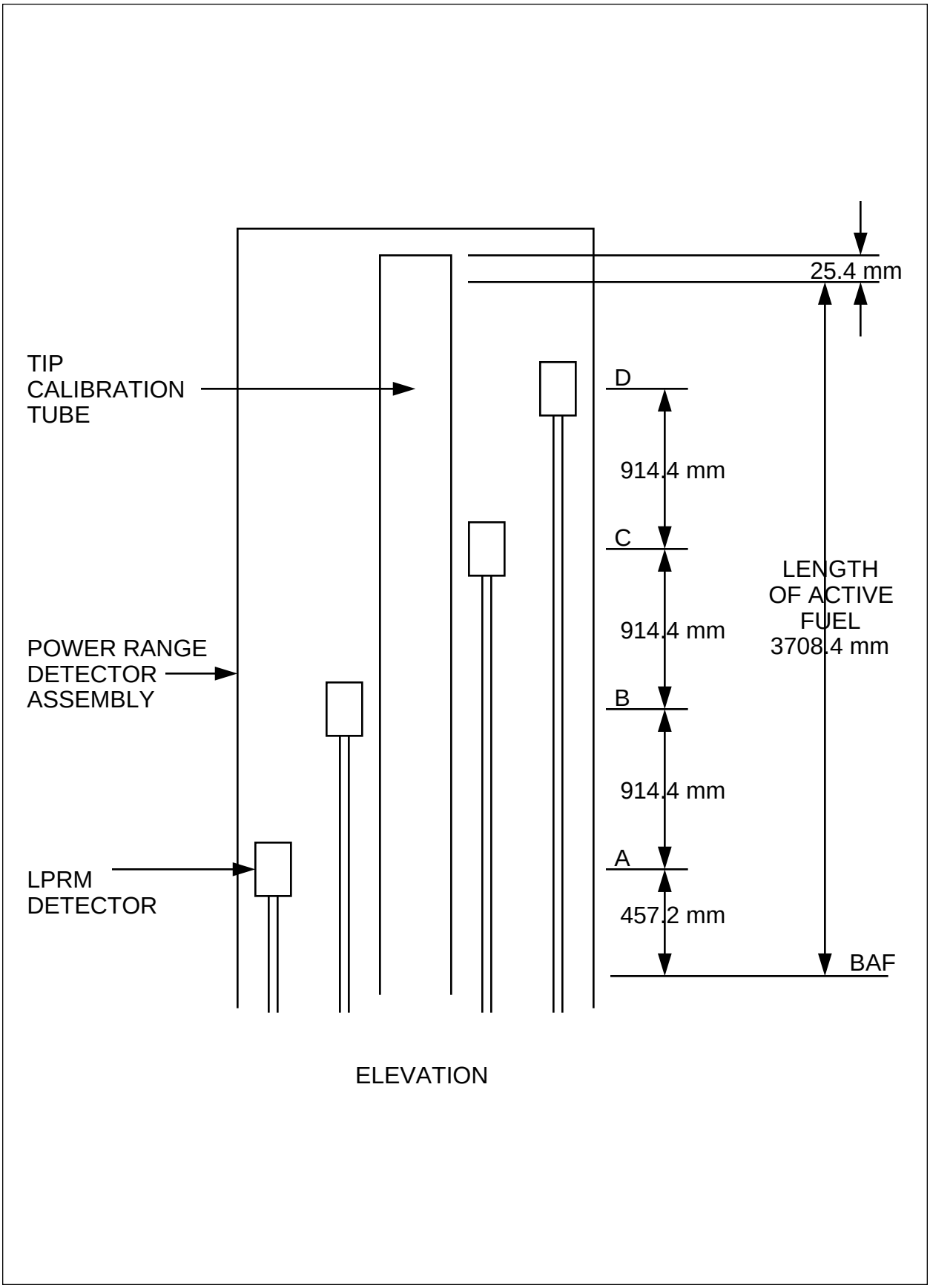



**Figure 7.6-3 LPRM Detector Location**

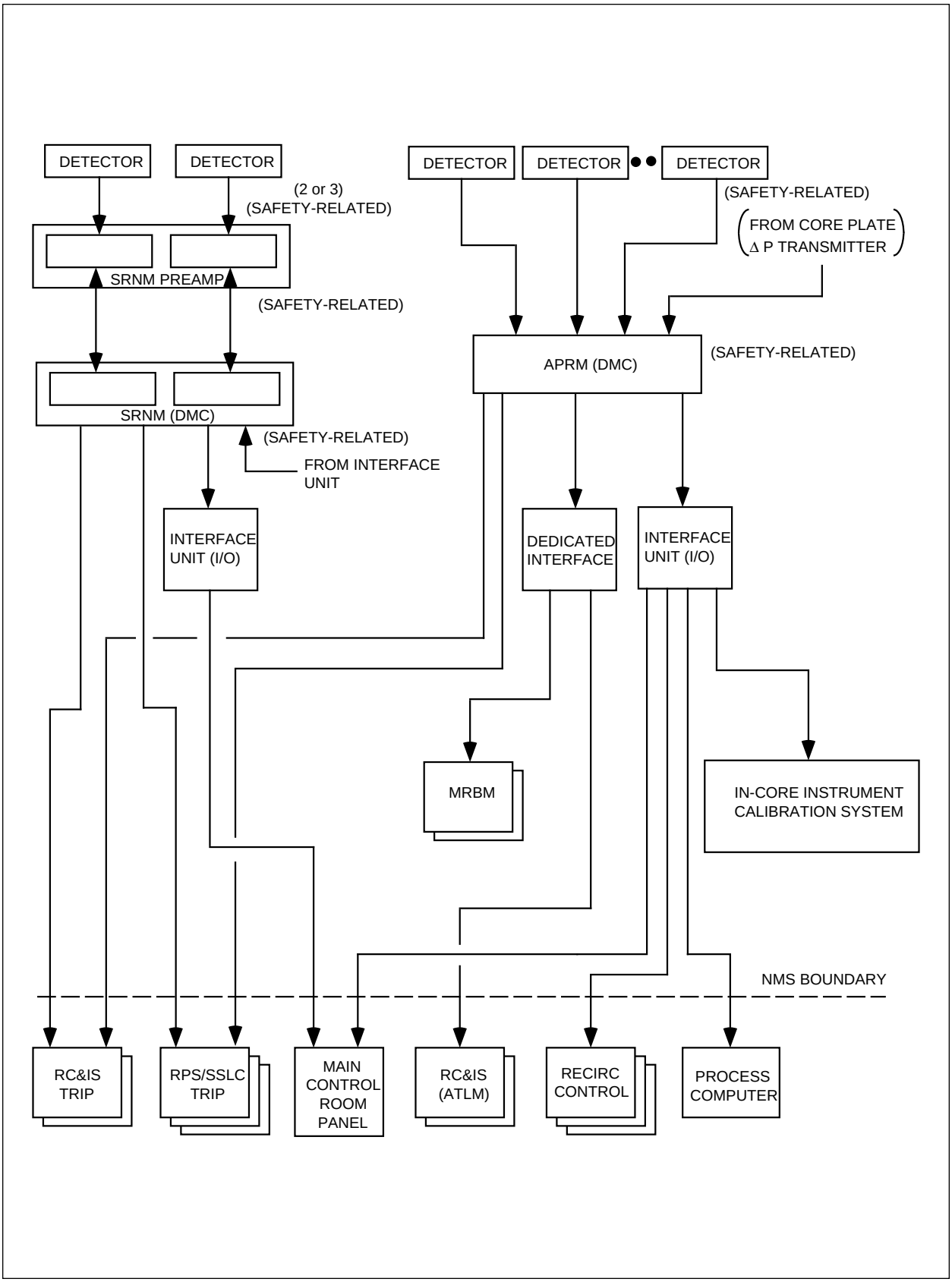



**Figure 7.6-4a**
**Basic Configuration of a Typical Neutron Monitoring System Division**

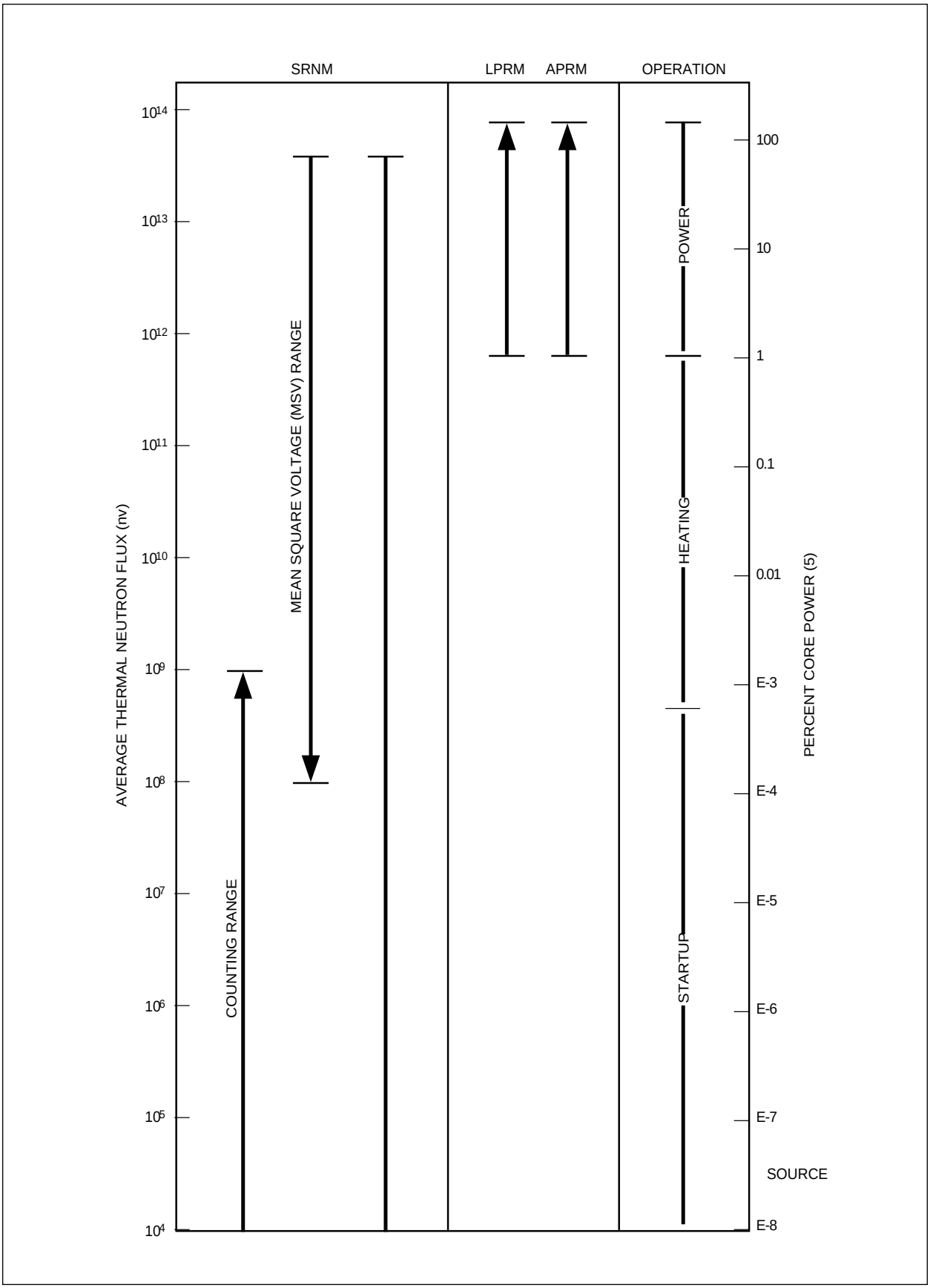



**Figure 7.6-4b Neutron Flux Monitoring Range**

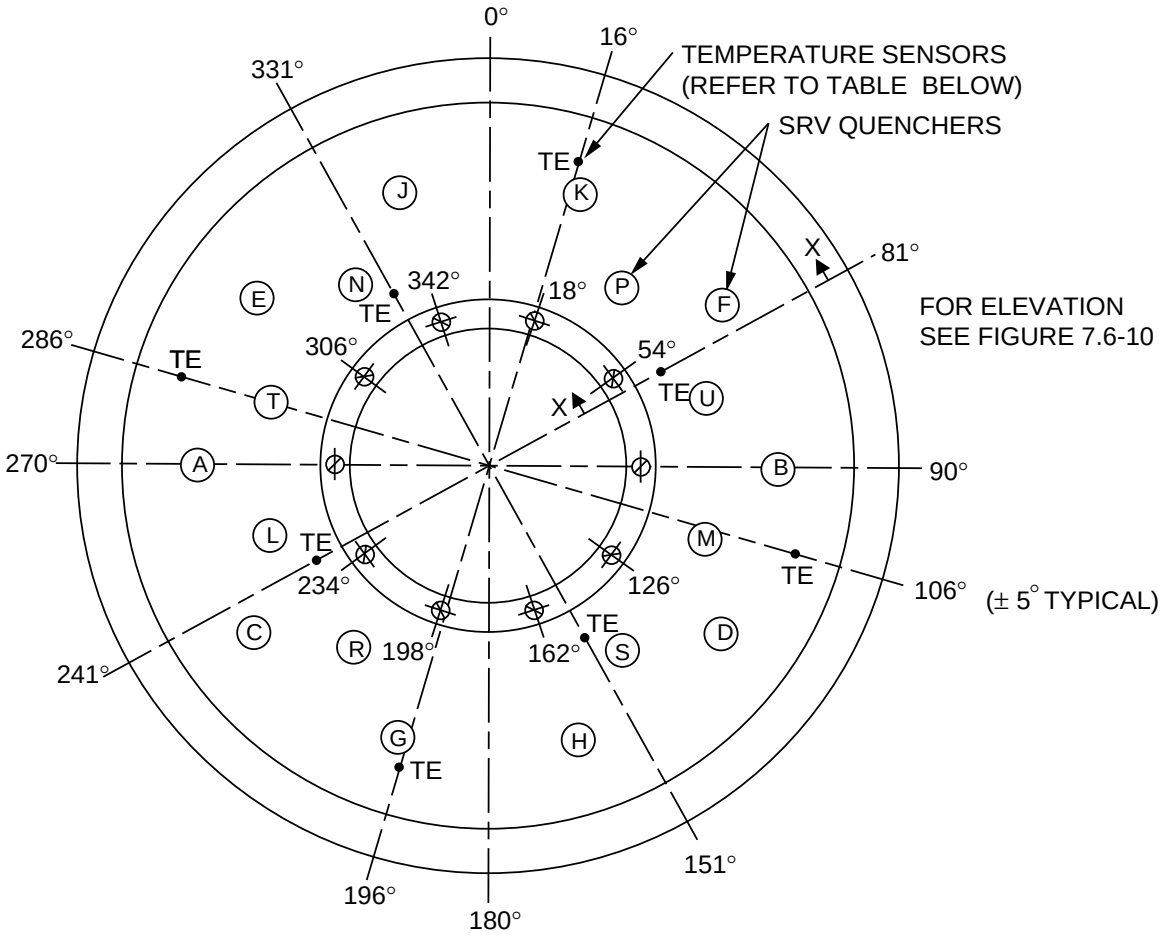
**The following figures are located in Chapter 21:**

**Figure 7.6-5 Process Radiation Monitoring System IED (Sheets 1-11)**

**Figure 7.6-6 Not Used**

**Figure 7.6-7 Containment Atmospheric Monitoring System IED (Sheets 1-4)**

**Figure 7.6-8 Containment Atmospheric Monitoring System IBD (Sheets 1-10)**




| | DIVISION I | DIVISION II | DIVISION III | DIVISION IV |
|---|---|---|---|---|
| 16° | TE-001A,E,J,N | | TE-001C,G,L,R | |
| 61° | | TE-002B,F,K,P | | TE-002D,H,M,S |
| 106° | | TE-003B,F,K,P | | TE-003D,H,M,S |
| 151° | TE-004A,E,J,N | | TE-004C,G,L,R | |
| 196° | TE-005A,E,J,N | | TE-005C,G,L,R | |
| 241° | | TE-006B,F,K,P | | TE-006D,H,M,S |
| 286° | | TE-007B,F,K,P | | TE-007D,H,M,S |
| 331° | TE-008A,E,J,N | | TE-008C,G,L,R | |

NOTE: DIVISIONS I, II, III AND IV TEMPERATURE SENSORS AT EACH LOCATION SHALL BE SEPARATED BY 15 – 30 CM.

**Figure 7.6-9 Instrumentation Location Definition for the Suppression Pool Temperature Monitoring System**

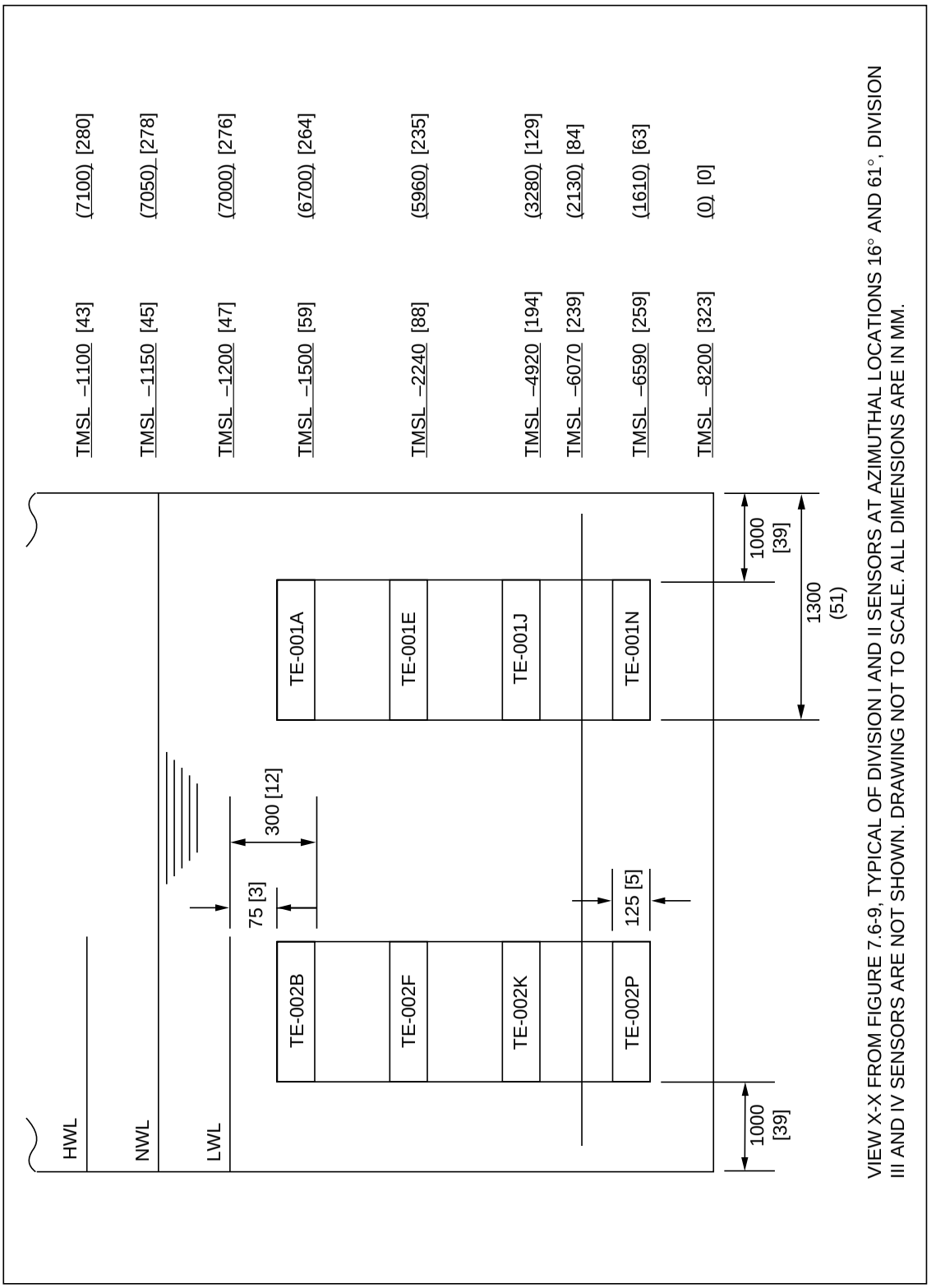



**Figure 7.6-10 Suppression Pool Temperature Monitoring System Sensor and Envelope Definition**

**The following figures are located in Chapter 21:**

**Figure 7.6-11 Suppression Pool Temperature Monitoring System IED (Sheets 1-3)**

**Figure 7.6-12 Suppression Pool Temperature Monitoring System IBD (Sheets 1–6)**

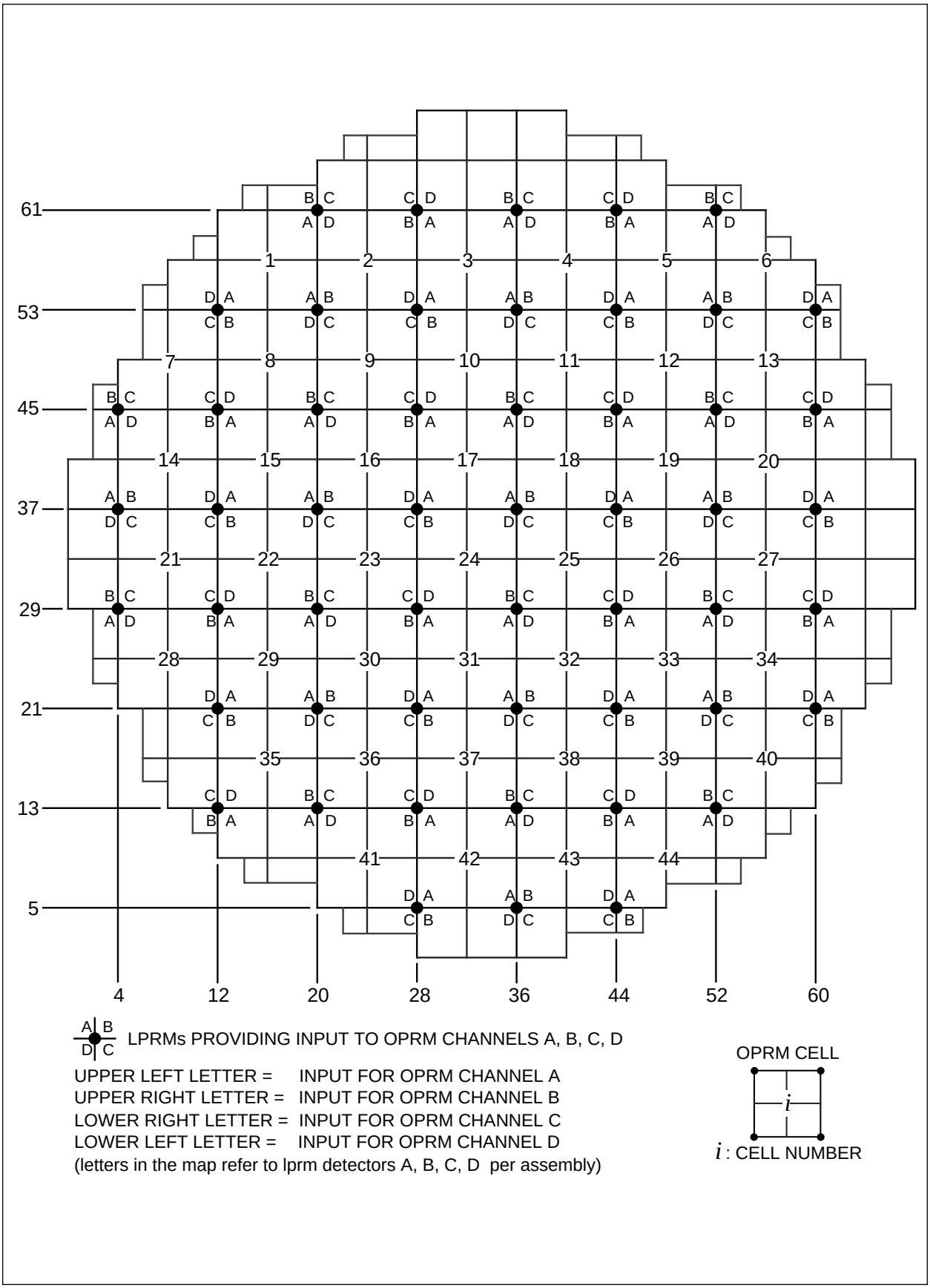



**Figure 7.6-13 LPRM Assignments to OPRM Channels**

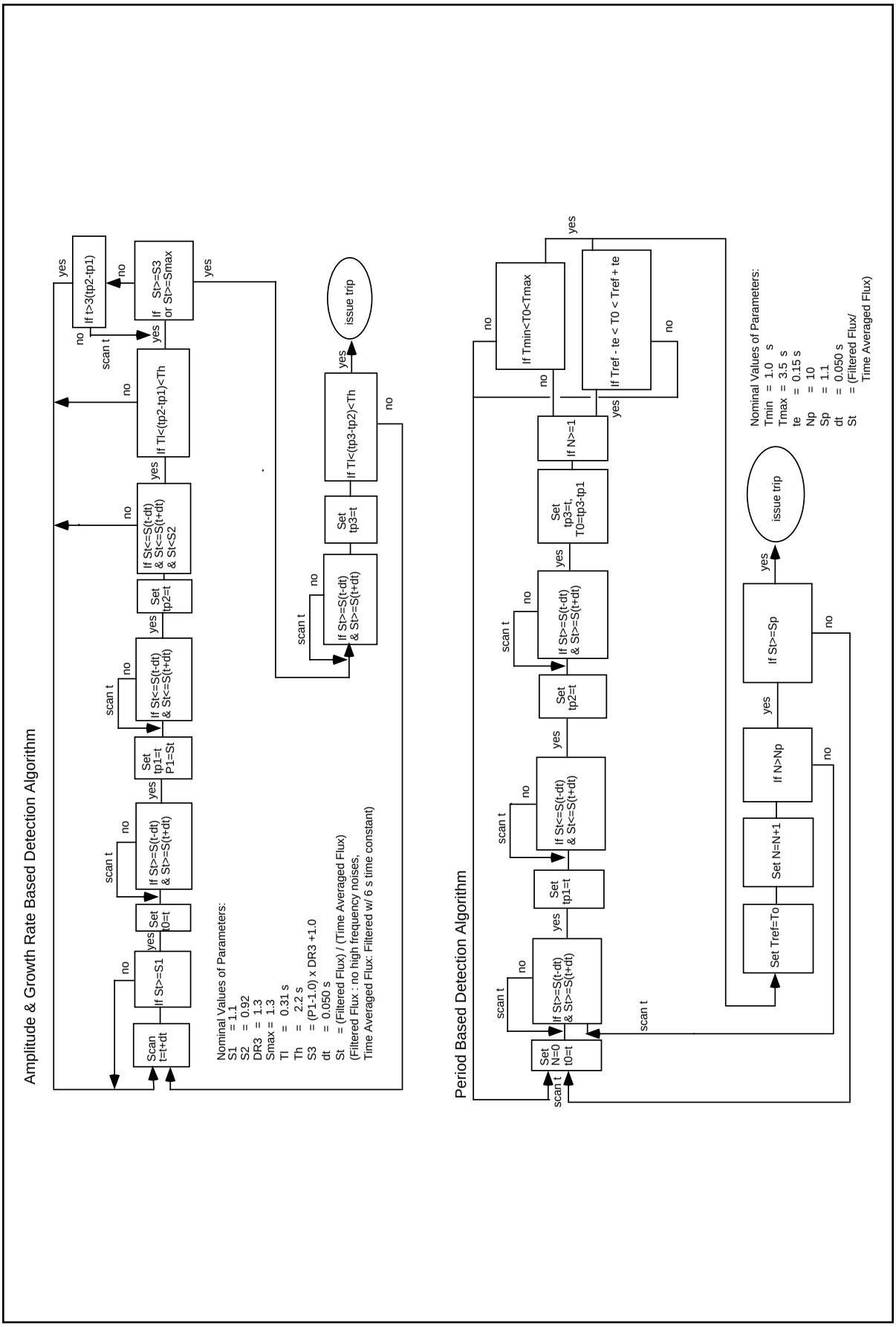



**Figure 7.6-14 OPRM Logic**

# 7.7 Control Systems Not Required for Safety

## 7.7.1 Description

This subsection provides discussion (or provides references to other chapter discussions) for instrumentation and controls of systems which are not essential for the safety of the plant, and permits an understanding of the way the reactor and important subsystems are controlled, and why failure of these systems does not impair safety functions. The systems include the following:

- Nuclear Boiler System—Reactor Vessel Instrumentation
- Rod Control and Information System
- Recirculation Flow Control System
- Feedwater Control System
- Process Computer System
- Neutron Monitoring System—ATIP Subsystem
- Automatic Power Regulator System
- Steam Bypass and Pressure Control System
- Non-Essential Multiplexing System
- Other Non-Safety Related Control System
- Fire Protection System (Chapter 9)
- Drywell Cooling System (Chapter 9)
- Instrument Air Systems (Chapter 9)
- Makeup Water System (Chapter 9)
- Atmospheric Control System (Chapter 6)
- Fuel Pool Cooling and Cleanup System (Chapter 9)

### 7.7.1.1 Nuclear Boiler System—Reactor Vessel Instrumentation

Figure 5.1-3 (Nuclear Boiler System P&ID) shows the instrument numbers, arrangements of the sensors, and sensing equipment used to monitor the reactor vessel conditions. The NBS interlock block diagram (IBD) is found in Figure 7.3-2. Because the NBS sensors used for safety-related systems, engineered safeguards, and control

systems are described and evaluated in other portions of this document, only the non-safety-related sensors for those systems are described in this subsection.

(1) System Identification

The purpose of the NBS instrumentation is to monitor and provide control input for operation variables during plant operation.

The non-safety-related instruments and systems are used to provide the operator with information during normal plant operation, or provide control input for non-safety-related functions.

(2) Classification

The systems and instruments discussed in this subsection are designed to operate under normal and peak operating conditions of system pressures and ambient pressures and temperatures and are classified as non-safety-related. However, mechanical interface of non-safety-related instruments with safety-related instrument piping is either classified as essential passive to avoid compromise of the Class 1E sensing capability (e.g., a pressure-containing body of a non-1E transmitter on a Class 1 instrument line is classified as essential passive and is environmentally qualified), or redundant sensing lines (four total) are provided with 2/4 safety system logic to show compliance with NRC Regulatory Guide 1.151.

(3) Power Sources

The non-safety-related instruments discussed in this subsection are powered from the non-Class 1E instrument buses.

(4) Equipment Design

For instruments which are located below the process tap, the sensing lines will slope downward from the process tap to the instrument, so that air traps are not formed.

Where it is impractical to locate the instruments below the process tap, the sensing lines descend below the process connection before sloping upward to a high point vent located at an accessible location.

The purpose of this is to permit venting of non-condensable gases from the sensing line during calibration procedures.

(5) Reactor Vessel Temperature

The reactor pressure vessel (RPV) coolant temperatures are determined by measuring saturation pressure (which gives saturation temperature), outlet flow temperature to the reactor water cleanup CUW unit, and bottom head

drain temperature. Reactor vessel outside surface temperatures are measured at the head flange and bottom head locations. Temperatures needed for operation and for compliance with the Technical Specification operating limits are obtained from these measurements. During normal operation, either reactor steam saturation temperature and/or the inlet temperatures of the reactor coolant to the CUW unit and the RPV bottom drain can be used to determine the vessel temperature.

(6) Reactor Vessel Water Level

Figure 7.7-1 shows the water level range and the vessel penetration for each water level range. The instruments that sense the water level are strictly differential pressure devices calibrated for a specific vessel pressure (and corresponding liquid temperature) conditions. For consideration of non-condensable gases in instrument lines, see Subsection 5.2.5.2.1(12). The following is a description of each water level range shown on Figure 7.7-1.

(a) Shutdown Water Level Range

This range is used to monitor the reactor water level during the shutdown condition when the reactor system is flooded for maintenance and head removal. The water level measurement design is the condensate reference chamber leg type. The zero of the instrument is the top of the active fuel and the instruments are calibrated to be accurate at 0 MPaG and 48.9°C water in the vessel. The two vessel instrument penetrations elevations used for this water level measurement are located at the top of the RPV head and the instrument tap just below the bottom of the dryer skirt.

(b) Narrow Water Level Range

This range uses the RPV taps at the elevation near the top of the steam outlet nozzle and the taps at an elevation near the bottom of the dryer skirt. The zero of the instrument is at the top of the active fuel and the instruments are calibrated to be accurate at the normal operating point. The water level measurement design is the condensate reference chamber type and uses differential pressure devices as its primary elements. The Feedwater Control System (Subsection 7.7.1.4) uses this range for its water level control and indication inputs.

(c) Wide Water Level Range

This range uses the RPV safety-related taps at the elevation near the top of the steam outlet nozzle and the taps at an elevation below the top of the active fuel. The zero of the instrument is the top of the active fuel and the instruments are calibrated to be accurate at the normal power operating point. The water level measurement design is the condensate

reference type and uses differential pressure devices as its primary elements.

(d) Fuel Zone Water Level Range

This range uses the RPV taps at the elevation near the bottom of the dryer skirt and the taps below the top of the active fuel (above the pump deck). The zero of the instrument is the top of the active fuel and the instruments are calibrated to be accurate at 0 PaG and saturated condition. The water level measurement design is the condensate reference type and uses differential pressure devices as its primary element.

(e) Reactor Well Water Level Range

This range uses the RPV tap below the top of the active fuel. The zero of the instrument is the top of the active fuel. The temperature and pressure condition that is used for the calibration is 0 MPaG and 48.9°C water in the vessel. The water level measurement design is the pressure device which measures static water pressure inside the vessel and converts to a water level indication. This range is used to monitor the reactor water level when the reactor vessel head is removed and the reactor system is flooded during the refueling outage.

The condensate reference chamber for the narrow range and wide range water level range is common as discussed in Section 7.3

The concern that non-condensable gasses may build-up in the water column in the reactor vessel reference leg water level instrument lines, i.e., the reactor vessel instrument lines at the elevation near the main steam line nozzles, has been addressed by continually flushing these instrument lines with water supplied by the Control Rod Drive (CRD) System.

Reactor water level instrumentation that initiates safety systems and engineered safeguards systems is discussed in Subsections 7.2.1 and 7.3.1. Reactor water level instrumentation that is used as part of the Feedwater Control System is discussed in Subsection 7.7.1.4.

(7) Reactor Core Hydraulics

A differential pressure transmitter indicates core plate pressure drop by measuring the core inlet plenum and the space just above the core support assembly. The instrument sensing line used to determine the pressure below the core support assembly attaches to the same reactor vessel tap that is used for the injection of the liquid from the Standby Liquid Control System (SLCS). An instrument sensing line is provided for measuring pressure above

the core support assembly. The differential pressure of the core plate is indicated locally and recorded in the main control room.

Another differential pressure device indicates the reactor internal pump developed head by measuring the pressure difference between the pressure above and below the pump deck.

(8) Reactor Vessel Pressure

Pressure indicators and transmitters detect reactor vessel internal pressure from the same instrument lines used for measuring reactor vessel water level.

The following list shows the subsection in which the reactor vessel pressure measuring instruments are discussed.

(a) Pressure transmitters and trip actuators for initiating scram, and pressure transmitters and trip actuators for bypassing the MSIV closure scram, are discussed in Subsection 7.2.1.1.

(b) Pressure transmitters and trip actuators used for RCIC and LPFL are discussed in Subsection 7.3.1.1.

(c) Pressure transmitters and recorders used for feedwater control are discussed in Subsection 7.7.1.4.

(d) Pressure transmitters that are used for pressure recording are discussed in Section 7.5.

(9) Pressure between the inner and outer reactor vessel head seal ring is sensed by a pressure transmitter. If the inner seal fails, the pressure at the pressure transmitter is the vessel pressure, and the associated trip actuator will trip and actuate an alarm. The plant will continue to operate with the outer seal as a backup, and the inner seal can be repaired at the next outage when the head is removed. If both the inner and outer head seals fail, the leak will be detected by an increase in drywell temperature and pressure.

(10) Safety/Relief Valve Seal Leak Detection

Thermocouples are located in the discharge exhaust pipe of the safety/relief valve. The temperature signal goes to a multipoint recorder with an alarm and will be activated by any temperature in excess of a set temperature signaling that one of the SRV seats has started to leak.

(11) Other Instruments

The feedwater temperature is measured and transmitted to the main control room.

The feedwater turbidity is monitored and the signal is transmitted to the main control room for recording.

(12) Testability

Pressure, differential pressure, water level, and flow instruments are located outside the drywell and are piped so that calibration and test signals can be applied during reactor operation, if desired.

(13) Environmental Considerations

There is no special environmental consideration for the instruments described in this subsection except as discussed in (2) above for pressure containing parts of sensors sharing instrument lines with safety-related instruments.

(14) Operational Considerations

The reactor vessel instrumentation discussed in this subsection is designed to augment the existing information from the engineered safeguards systems instrumentation and safety system such that the operator can start up, operate at power, shut down, and service the reactor vessel in an efficient manner. None of this instrumentation is required to initiate any engineered safeguard or safety-related system and its failure will not disable any ESF or safety-related system.

(15) Reactor Operator Information

The information that the operator has at his disposal from the instrumentation discussed in this subsection is discussed below:

(a) The shutdown range water level, narrow range water level, wide range water level, fuel zone water level, and reactor well water level are indicated in the main control room.

(b) The core plate differential pressure provides a signal to the process computer.

(c) The reactor internal pump differential pressure is indicated in the main control room.

(d) The reactor pressure is indicated in the main control room and at two local racks in the containment by a pressure gauge.

(e) The reactor head seal leak detection system provides pressure indications in the control room and turns on an annunciator if the inner reactor head seal fails.

(f) The discharge temperatures of all the safety/relief valves are shown on a multipoint recorder in the control room. Any temperature point that has exceeded the trip setting will turn on an annunciator, indicating that a SRV seat has started to leak.

(g) Feedwater turbidity is recorded in the main control room. The recorder will turn on an annunciator in the main control room for either a high or low signal.

(16) Setpoints

The annunciator alarm setpoints for the reactor head seal leak detection, SRV seat leak detection, and feedwater corrosion product (turbidity) monitor are set so the sensitivity to the variable being measured will provide adequate information.

Tables 2 and 3 of Figure 5.1-3 show the relative indicated water levels at which various automatic alarms and safety actions are initiated. The following list tells where various level measuring functions are discussed and their setpoints are referenced.

(a) Level transmitters and trip actuators for initiating scram are discussed in Subsection 7.2.1.1.

(b) Level transmitters and trip actuators for initiating containment or vessel isolation are discussed in Subsection 7.3.1.2.

(c) Level transmitters and trip actuators used for initiating HPCF, RCIC, LPFL and ADS and the level actuators used to shut down the HPCF pump and RCIC turbine are discussed in Subsection 7.3.1.1.

(d) Level trips to initiate various alarms and trip the main turbine and the feedpumps are discussed in Subsection 7.7.1.4

### 7.7.1.2 Rod Control and Information System—Instrumentation and Controls

(1) System Identification

The main objective of the Rod Control and Information System (RCIS) is to provide the capability to control the fine motion control rod drive (FMCRD) motors of the Control Rod Drive (CRD) System (explained in Sections 4.6.1 and 4.6.2) to permit changes in core reactivity so that reactor power level and power distribution can be controlled.

The RCIS performs the following functions:

(a) Controls changes to the core reactivity, and thereby reactor power, by moving neutron absorbing control rods within the reactor core as initiated by:

  (i) The plant operator, when the RCIS is placed in manual or semiautomatic mode of operation

  (ii) The Power Generation and Control System (PGCS) when the PGCS, automatic power regulator (APR), and RCIS are in automatic mode

(b) Provides summary display information for the plant operator, indicative of aggregated control rod positions, status of the control rods, and the FMCRDs on the RCIS dedicated operator interface (DOI).

(c) Provides FMCRD status and control rod position and status data to other plant systems which require such data (e.g., the plant process computer system).

(d) Provides for automatic control rod run-in of all operable control rods following a scram.

(e) Automatically enforces rod movement blocks to prevent potentially undesirable rod movements (these blocks do not impact a scram insertion function).

(f) Provides the capability for insertion of all rods by an alternate and diverse method, based on receiving a command from the Recirculation Flow Control System (RFCS). This function is called the alternate rod insertion (ARI) function.

(g) Provides for insertion of selected control rods for core thermal-hydraulic stability control or for mitigation of a loss of feedwater heating event; called the selected control rod run-in (SCRRI) function, based on receiving SCRRI command from the RFCS.

(h) Insures that the pattern of control rods in the reactor is consistent with specific control rod pattern restrictions. This function is performed by the Rod Worth Minimizer (RWM) Subsystem of the RCIS and is effective only when reactor power is below the low power setpoint.

(i) Enforces fuel operating thermal limits (MCPR and MLHGR) when reactor power is above the low power setpoint. This function is performed by the Automated Thermal Limit Monitor (ATLM) Subsystem of the RCIS.

(j) Initiates the "Run Back" signals to adjustable speed drives (ASDs) of the Recirculation Flow Control System, through hard-wire connections to ASDs, whenever an all-rods-in condition is detected in the RCIS.

(k) Provides the capability for conducting FMCRD-related surveillance tests.

(l) Through the capabilities of the Gang Rod Selection and Verification Logic of the Rod Action and Position Information, enforces adherence to a predetermined rod pull/insert sequence, called the reference rod pull sequence (RRPS).

The RCIS IED is shown in Figure 7.7-2. This drawing depicts the major components of the RCIS, their interconnections and interfaces with other ABWR systems.

(2) System Description

The RCIS is a dual redundant system consisting of two independent channels for normal monitoring of control rod positions and executing control rod movement commands. Each channel receives separate input signals and both channels perform the same function. Disagreement between the two channels results in rod motion inhibit.

The RCIS consists of several different types of cabinets (or panels), which contain special electronic/electrical equipment modules and a dedicated operator interface on the main control panel in the control room. There are four types of electronic/electrical cabinets that make up the RCIS:

(a) Rods Action Control Cabinet (RACC)

There are two RACCs consisting of RACC-Channel A and RACC-Channel B, that provide for a dual redundant architecture. Each RACC subsystem consists of three main functional subsystems, as follows:

(i) Automated Thermal Limit Monitor (ATLM)

(ii) Rod Worth Minimizer (RWM)

(iii) Rod Action and Position Information (RAPI)

(b) Remote Communication Cabinets (RCC)

The RCCs contain a dual channel file control module (FCM) that interfaces with the rod server modules (RSMs) that are contained in the same cabinets, and RAPI in the control room.

(c) Fine Motion Driver Cabinets (FMDC)

The FMDCs consist of several inverter controllers (IC) and stepping motor driver modules (SMDM). Each SMDM contains an electronic converter/inverter to convert incoming three-phase AC power into DC and inverts the DC power to variable voltage/frequency power pulses for the FMCRD stepping motor.

(d) Rod Brake Controller Cabinets (RBCC)

The RBCCs contain electrical and/or electronic logic and other associated electrical equipment for the proper operation of the FMCRD brakes. Signals for brake disengagement or engagement are received from the associated rod server module, and the brake controller logic provides two separate (channel A and channel B) brake status signals to its corresponding rod server module.

(3) The RCIS Multiplexing Network

The RCIS multiplexing network consists of two independent channels (A and B) of fiber-optic communication links between the RACCs (channels A and B), and the dual channel file control modules located in the remote communication cabinets.

The plant essential multiplexing network interfaces with FMCRD dual redundant separation switches (A/B) and provides the appropriate status signals to the RACCs to be used in the RCIS logic for initiating rod block signals if a separation occurs. The essential multiplexing network is not part of the RCIS.

(4) Classification

The RCIS is not classified as a safety-related system, as it has a control design basis only and is not required for the safe and orderly shutdown of the plant. A failure of the RCIS will not result in gross fuel damage. The rod block function of the RCIS, however, is important in limiting the consequences of a rod withdrawal error during normal plant operation. An abnormal operating transient that might result in local fuel damage is prevented by the rod block function of the RCIS.

The RCIS is single-failure proof with high reliability and availability. In accordance with the non-safety-related system application procedure section of the plant general system application requirement document, the RCIS is classified as a non-safety-related, Class 3, power generation system.

(5) Power Sources

(a) Normal

The incoming three-phase AC power for the stepping motor driver modules and the rod brake controller power supplies is derived from the Division I Class 1E AC power bus.

The power for all RCIS equipment, except as noted above, is derived from two separate, nondivisional uninterruptible AC power sources (UPS) (Subsection 8.3.1 and 8.3.1.1.4).

Each of the two RACCs has redundant auxiliary electrical power supplies and cooling fans, as required, for proper operation of their associated subsystems.

The RCC contains the necessary redundant power supplies for channels A and B of the rod server modules, file control modules, electrical equipment, and cooling fans (if required).

(b) Alternate

On loss of normal auxiliary power, the Division I station diesel generator provides backup power to Division I Class 1E bus.

(6) RCIS Scope

The RCIS scope includes the following equipment:

(a) All the electrical/electronic equipment contained in the RACCs, the RCCs, the FMDCs, and the RBCCs.

(b) The RCIS multiplexing network equipment.

(c) The cross-channel communication link between the two RACS channels.

(d) The dedicated RCIS operator's interface and the communication links from the equipment to this interface.

(7) Integral Functional Design

The following discussion examines the control rod movement instrumentation and control aspects of the subject system and the control rod position information system aspects. The "control" description includes the following:

— Control Rod Drive System—control

— Control rod drive—hydraulic system

— Rod movement and rod block logic—RCIS

Figure 7.7-4 shows the interlock block diagram of the Control Rod Drive System. Figure 7.7-2 shows the IED for the RCIS. The interlock block diagram (IBD) for the RCIS is shown in Figure 7.7-3. Figure 4.6-8 shows the layout of the CRDHS.

The Control Rod Drive System is composed of three major subsystems: (1) the fine motion control rod drive (FMCRD), including the stepping motors and instrumentation for monitoring rod position and the brake, (2) the hydraulic control units (HCU), and (3) the Control Rod Drive Hydraulic System (CRDHS).

The Control Rod Drive (CRD) System performs the following functions:

(a) Controls gross changes in core activity by electromechanical positioning of neutron-absorbing control rods within the core in response to electrical power pulses for the control of stepping motors. These power pulses are received from the RCIS.

(b) Gathers rod status and rod position data, and provides signals for logic control and performance monitoring to the RCIS.

(c) Provides for rapid control rod insertion (scram) so that no fuel damage results from any abnormal operating transient. This function is independent of the RCIS.

(d) Provides for electromechanical insertion of selected control rods for core thermal/hydraulic stability control.

(e) Provides for insertion by an alternate and diverse method, of all control rods on receipt of an ATWS (anticipated transient without scram) signal.

The CRD System components which are required for the orderly shutdown of the plant are designed to meet requirements for a safety-related system. The components that are required for positioning the control rods to control power generation meet the design requirements of a control system. The RCIS classification is identified under Subsection 7.7.1.2 (4).

The control rods are moved by (1) the fine motion control rod drive (FMCRD) motors (motor-driven positioning) for normal insertion and withdrawal of the control rods on receiving drive motion signals from the RCIS and (2) hydraulic-powered rapid control rod insertion (scram) for abnormal operating conditions in response to signals received from the Reactor Protection System.

The hydraulic power required for scram is provided by high pressure water stored in individual Hydraulic Control Units (HCUs) and each HCU contains a nitrogen gas/water accumulator charged to a high pressure along with the necessary valves and components to scram two control rods except for the one HCU that is connected to only one control rod.

#### 7.7.1.2.1 Control Rod Drive Control System Interfaces

(1) Introduction

When an operator selects a control rod for motion (Figure 7.7-3), the operator first selects the manual rod movement mode at the dedicated RCIS operator panel, by depressing the manual mode switch to place the RCIS in manual mode. Then the operator depresses the select pushbutton for either single rod movement or for ganged rod movement. The operator must then select a specific rod (or a gang) to be moved at the normal operational manual mode CRT display under the control of the Performance Monitoring and Control System (PMCS).

A CRT display generated by PMC presents to the operator a full core array of all 205 control rods in addition to 52 local power range monitors (LPRMs) schematically as a group of boxes.

Each box represents a control rod containing the core coordinates and vertical rod position of that rod in white numbers on a black background. The vertical rod position information is normally not visible but becomes visible in response to actuation of various rod status and position requestor poke points. The core coordinates are always visible to the operator.

The CRT display provides the operator with a capability to move a single rod or a ganged selection. For this discussion, the operator selects a single rod for withdrawal. Four rod movement commands (poke points) serve as a means to initiate all rod movements controlled from this display. They are identified as “SINGLE ROD”, “ROD GANG”, “STEP” or “CONTINUOUS”, and “IN” or “OUT”.

The operator first identifies the rod status from the rod status requestor information display, then makes a decision for either a withdrawal or an insertion of a control rod and sets up the display. The operator can request rod status information by actuating poke points on the CRT for the required rod.

(2) Withdrawal Cycle

Following is a description of steps the operator performs at the RCIS dedicated operator's interface panel in selecting a rod for movement in the manual mode. The operator depresses the manual rod movement mode switch, which enables the RCIS for manual mode. The operator then verifies indicator / alarm status at the control panel for the following conditions:

(a) Reactor power level is below low power setpoint (LPSP).

(b) Manual rod movement indicator is illuminated.

(c) Verifies status of channel bypass conditions for RWM, RACS, and ATLM.

(d) RCIS trouble indicator is not illuminated.

(e) RCIS rod block status indicator is not illuminated.

(f) No audible alarms are present.

(g) Verify status of FMCRDs, for number rods, in "Full In" or "Full Out", "Latched Full In", or in an "Inoperable Bypass" condition.

Following is a description of steps an operator performs at the PMCS CRT display in selecting a single rod for continuous withdrawal with RCIS initially in manual mode. The detailed operations between the RCIS and the CRD System with specific response when various commands are transmitted are discussed.

The setup at the CRT display for continuous withdrawal of a single control rod is as follows:

— With top level CRT display, the operator requests the display of rod position data by actuating the rod position data poke points. The screen display changes to the RCIS normal operation / manual mode screen and shows all control rods and their positions. The screen display has other poke points for operating in the manual mode.

— Under rod command display, if it shows "IN" and "STEP", the operator can change the setup. A touch of "IN" poke point changes it to "OUT" and a touch of the "STEP" poke point changes it to "NOTCH" or to "CONTINUOUS" if "NOTCH" is touched. After proper selections are verified, the operator can then select the single rod by actuating the poke points for a "SINGLE ROD". The operator verifies the selections by observing the status indicators. The operator then follows up by touching the display array box representing the rod (ROD SELECTED) to be moved.

This setup and action by the operator sends rod coordinates and other setup data to the PMCS. The data representing a single rod to be withdrawn is coded and stored in PMCS memory. The PMCS addresses the RCIS and sends the coded messages. The coded messages are received at the RCIS and stored in the Rod Position and Information Subsystem memory. The operator has an option to stop the rod movement by using the light pen. Touching the "SINGLE ROD" poke point a second time causes rod motion stop signals to be sent to the RCIS interface.

The information displayed to the operator at this time is the vertical position of the rod selected and it remains displayed until a new selection is made or the rod is deselected. The display array boxes representing all other rods in the core at this time dim to approximately half brightness.

The CRT display stores information in memory during the initial setup and transmits the information to the PMCS. When the operator initializes the last poke point (ROD SELECTED), the information stored in memory addressing the manual rod movement command signals in the PMCS are downloaded, as two independent signals, into channels A and B of the RCIS Rod Action and Position Information (RAPI) Subsystems.

The RCIS receives the two independent streams of data signals transmitted from the PMCS. The data are received and loaded into memory at the RAPI Subsystems (channel A/B). Both channel A/B are identical and perform the same functions. If there is a disagreement between A and B, the logic issues a rod motion inhibit signal. The operator has the capability to bypass certain functions in the manual mode.

The PMCS also sends data to the Automated Thermal Limit Monitor (ATLM) of the RCIS on the calculated fuel thermal operating limits and corresponding initial LPRM values when an ATLM setpoint update is requested.

The logic of the ATLM subsystem issues a rod block signal that is used in the RAPI System logic to enforce a rod block that prevents violation of the fuel thermal operating limits. The ATLM interfaces with and receives signals from the RAPI Subsystem control logic for rod position data, other plant data and control signals.

The ATLM interfaces with Recirculation Flow Control (RFC) System and when it trips, a signal is sent to the RFCS which would cause a flow increase block.

The ATLM also receives input signals, based upon the LPRMs and APRMs of the Neutron Monitoring System (NMS). The RAPI Subsystem logic enforces

ATLM rod block signals to the RCIS rod server modules located in the remote communication cabinets. Either channel of an ATLM subsystem can independently cause a rod withdrawal block.

The Rod Worth Minimizer (RWM) Subsystem logic issues rod block signals that are used in the Rod Action Control Subsystem rod block logic to assure that absolute rod pattern restrictions are not violated (e.g., the ganged withdrawal sequence restrictions). The logic of the RWM also receives rod position data and control status signals from the logic of the RAPI Subsystem and feeds back RWM status signals.

The RCIS responds to data signals originating from the CRT displays of the PMCS for operator requested rod withdrawal or insertion commands.

The RAPI Subsystem of the RCIS enforces rod blocks based upon signals internal or external to the system.

The internal signals include those signals from any of the above MRBM, ARBM, RWM. If there is any disagreement between the two channel logic of the RAC and/or the RAPI subsystems of the RCIS, rod block signals are transmitted to the rod server module and sent to the PMCS.

External input signals which could cause rod blocks originate from the SRNM and PRNM Subsystems or from the four divisions of the essential multiplexing system, reflecting the status of separation switches of the FMCRDs.

After performing the required validity checks within each subsystem and verifying that there are no rod block conditions existing, the RAPI Subsystem of the RCIS transmits command data signals (representing the selection of a single rod for withdrawal via the RCIS multiplexing system channel A and channel B) to a dual channel file control module (FCM) located in a remote communication cabinet. The selected rod command withdrawal signals are received at the dual channel FCM and routed via channel A and channel B of the dual channel rod server modules (RSMs) and then are loaded into data buffers A and B of the inverter controller.

The FCM also interfaces with instrumentation of the FMCRD (a subsystem of the control rod drive system), collects data associated with the position reed switches and converts the synchro A and synchro B analog data into digital data for use in the RSM logic and transmission (via the RCIS multiplexing system) to the RAPI Subsystem logic.

The RSM, which consists of two rod server processing channels and one inverter controller, interfaces with the rod position instrumentation through

its two processing channels and with the associated stepper motor driver module of the FMCRD System via the inverter controller. After receiving the proper command signals for a single rod to be withdrawn continuously, the inverter controller sends the proper motor power control information to the stepper motor driver module. In turn, the stepper motor driver module sends power pulses to the FMCRD motor.

Each of the rod server processing channels A and B also interfaces with the rod brake controller to provide brake disengagement and / or engagement signals required for normal rod movement. This is based on two-out-of-two logic where both channels A and B of the RSM should agree, and on one-out-of-two logic for ARI and scram following functions.

Each rod server processing channel of the RCIS obtains rod position status information signals via hardwired interfaces with its associated FMCRD synchro and obtains additional rod position and status information via hardwired interfaces with the reed switches included in the FMCRD. The reed switch based position signals are mainly used for recording FMCRD scram timing analysis data. Each rod server processing channel exchanges the continuous synchro position information and transmits the data to the RAPI Subsystem of the RCIS for usage in its logic. This data is also used to provide position status signals to the PMCS and to the RCIS dedicated interface panel.

(3) Insert Cycle

An operator action to insert a rod while in the manual mode would be processed in a similar manner as above, except that signals for an insertion of the rod would be decoded at the rod server module (RSM). On receiving the correct signals from the RSM, the stepper motor driver module would provide power pulses to the FMCRD motor such that control rod insertion would result.

(4) Ganged Rod Motion

There are three means of controlling ganged rod motion. The RCIS provides for automatic mode, semi-automatic, and manual mode. When in the automatic mode of operation, commands for reactivity insertion or withdrawal are received from the Automatic Power Regulator (APR) System.

The RCIS dedicated operator interface provides switches for an automatic, semi-automatic, or manual rod movement mode of operation. When the system is in semi-automatic mode, all rod movements are controlled by the operator. However, the RCIS, by using a database called reference rod pull

sequence (RRPS) and keeping track of the current control rods' positions, prompts the operator to the selection of the next gang.

When the RCIS is in manual mode and ganged rod movement mode has also been chosen, if the operator selects a specific rod in a gang, the logic will automatically select all associated rods in that gang.

When the automatic mode is active, the RCIS responds to signals for rod movement request from the APR System. In this mode, the APR simply requests either reactivity insertion or withdrawal. The RCIS responds to this request by using the RRPS and the current rods' positions and automatically selects and executes the withdrawal/insert commands for the next gang.

In order for the automatic rod movement feature of the RCIS to be active, the power generation control system must be in the automatic mode, the automatic power regulator system must be in the automatic mode, and the switch on the RCIS dedicated operator interface for automatic rod movement mode must be depressed. The operator has an option of discontinuing the automatic operation by placing either the PGCS/APR or RCIS mode switches back to manual mode.

(5) Ganged Withdrawal Sequence Restrictions

The RWM of the RCIS ensures adherence to certain ganged withdrawal sequence restrictions by generating a rod block signal for out-of-sequence rod withdrawals. These types of restrictions are specified as follows:

(a) The ganged rod mode consists of one or two sets of fixed control rod gang assignments. The two sets of rod gang assignments correspond to sequences A and B of the ABWR ganged withdrawal sequence, as specified in the reactivity control document.

(b) The system allows up to 26-rod gangs, for control rods in rod groups 1, 2, 3, and 4, to be withdrawn simultaneously when the reactor is in the startup mode. These withdrawals are permitted only under the following conditions:

(i) Reactor power level is below the low power setpoint (LPSP).

(ii) A group 1, 2, 3, or 4 gang of rods is selected. Only one group at a time is allowed for normal rod movement.

(iii) Groups 1-4 may only be withdrawn before groups 5-10 are in the full-in position.

(iv) The other three groups (of groups 1-4) that are not selected must be either full-in or full-out. Groups 1-4 are withdrawn from the full-in position to the full-out position before another group is moved.

(v) The chosen alternative sequence for withdrawing the first four groups is consistent with one of the following allowable alternate sequences:

(a) (1, 2, 3, 4)

(b) (1, 2, 4, 3)

(c) (2, 1, 3, 4)

(d) (2, 1, 4, 3)

(e) (3, 4, 1, 2)

(f) (3, 4, 2, 1)

(g) (4, 3, 1, 2)

(h) (4, 3, 2, 1)

No sequences other that those indicated above are allowed within the logic of the RCIS. The logic of the RCIS also ensures that, when single rod movements of rods in groups 1-4 are made, they are in accordance with the above restrictions (e.g., if one of the rods from group 1 is withdrawn, all the other group 1 rods are to be withdrawn before withdrawal of rods in another group is permitted).

(vi) The RCIS logic enforces additional ganged withdrawal sequence restrictions when the reactor power level is below the low power level setpoint as follows:

(a) The RCIS logic prevents two groups of rods from being withdrawn simultaneously.

(b) Allows only groups 1-6 to be withdrawn as one single gang.

(c) Assures that the maximum allowable difference between the leading and trailing operable control rods in each of groups 3, 4, 7, 8, 9, and 10 to be within 146 mm when any operable rod in the group is less than or equal to 0.914m withdrawn. This restriction is not applied to groups 1, 2, 5, and 6 or to any group when all operable rods in that group are greater

than 0.914m withdrawn. This restriction applies to rod pull sequence (5)a through (5)d above.

(d) Assures that the maximum allowable difference between the leading and trailing operable control rods in each of groups 1, 2, 7, 8, 9, and 10 to be within 146.4 mm when any operable rod in the group is less than or equal to 0.914m withdrawn. This restriction is not applied to groups 3, 4, 5, and 6 or to any group when all operable rods in that group are greater than 0.914m withdrawn.The restriction applies to rod pull sequence (5)e through (5)h above.

(e) Enforces restrictions on withdrawal of rods in groups 5-10 if rods in group 7 or 8 are moved first. Movement of rod gangs in groups 9 and 10 are then blocked until all operable rods in groups 5, 6 and 7 or 8 are greater or equal to 0.914m withdrawn. The RCIS also enforces rod restrictions if rods in group 9 or 10 are moved first. Movement of rod gangs in groups 7 and 8 is blocked until all operable rods in group 5, 6 and 9 or 10 are greater than or equal to 0.914m withdrawn.

(6) Establishment of Reference Rod Pull Sequence (RRPS)

The reference rod pull sequence is normally established before plant startup and stored in memory at the Performance Monitoring and Control System (PMCS). The PMCS allows modifications to be made to the RRPS through operator actions. The PMCS provides compliance verification of the changes to the RRPS, with the ganged withdrawal sequence requirements.

The RCIS provides a capability for an operator to request a download of the RRPS from the PMCS, a subsystem of the Process Computer System. The new RRPS data is loaded into the RAPI System. Download of the new RRPS data can only be completed when the RCIS is in manual rod movement mode and when both keylock permissive switches located at each rod action control cabinet are activated.

The RCIS provides feedback signals to the PMCS for successful completion of downloaded RRPS data for displaying on the CRT display.

Rod withdrawal block signals are generated whenever selected single or ganged rod movements differ from those allowed by the RRPS, when the RCIS is in automatic or semi-automatic rod movement mode.

The RCIS sounds an audible alarm at the operators panel for a RRPS violation.

(7) Rod Block Function

The rod block logic of the RCIS, upon receipt of input signals from other systems and internal subsystems, inhibits movement of control rods.

All Class 1E systems rod block signals to the RCIS are optically isolated. The rod block signals change the state of the light emitting diode at the external interface of an isolator. The light crosses the boundary of the isolator to the interface of the RCIS where a photo transistor changes state, thereby communicating the information to the logic within the RCIS. This provides complete isolation while keeping electrical failures from propagating into the RCIS and vice versa.

The presence of any rod block signal, in either channel or both channels of the RCIS logic, causes the automatic changeover from automatic mode to manual mode. The automatic rod movement mode can be restored by taking the appropriate action to clear the rod block and by using the selector switch to restore the automatic rod movement mode.

If either channel or both channels of the RCIS logic receive(s) a signal from any of the following type of conditions, a rod block is initiated:

(a) Rod separation, only for those rod(s) for which separation is detected.

(b) Reactor in SHUTDOWN mode (all control rods).

(c) SRNM period alarm (all control rods, but not applicable when reactor in RUN mode).

(d) SRNM downscale alarm or SRNM upscale alarm or APRM set down upscale alarm (all control rods, but not applicable when in RUN mode).

(e) SRNM inoperative (all control rods, but not applicable when reactor is in RUN mode).

(f) APRM downscale (all control rods, only applicable when reactor in RUN mode).

(g) Flow-biased APRM rod block (all control rods, only applicable when reactor in RUN mode).

(h) APRM inoperative (all control rods, only applicable when reactor in RUN mode).

(i) Low CRD charging header pressure (all control rods).

(j) Low CRD charging header pressure trip function bypass switches of the reactor protection system are in a bypass position (all control rods).

(k) Violation of ganged withdrawal sequence restrictions (all control rods in the selected gang or the selected control rod if the single rod movement mode is being used; applicable below the low power setpoint).

(l) Automated Thermal Limit Monitor (ATLM) rod block (all control rods, only applicable above the low power setpoint).

(m) Multi-channel Rod Block Monitor (MRBM) rod block (all control rods, only applicable above the low power setpoint).

(n) ATLM trouble (all control rods, only applicable above the low power setpoint).

(o) RWM trouble (all control rods, applicable below the low power setpoint).

(p) MRBM inoperative (all control rods, only applicable above the low power setpoint).

(q) Rod action position information trouble (all control rods).

(r) Two or more recirculation pump trips when reactor power is above approximately 25% of rated and core flow is below approximately 36% or rated. The logic to generate this rod block resides in the RFCS and the discrete rod block signal is sent to the RCIS from the RFCS.

(s) Refueling platform control computer interlock rod block (all control rods, only applicable when the reactor is in the refuel mode).

(t) Reactor SCRAM condition exists (all control rods).

(u) Existence of ARI or SCRRI condition (all control rods).

(v) Gang misalignment [i.e. position difference between any two gang members of more than 38.1 mm (all control rods)].

The RCIS enforces all rod blocks until the rod block condition is cleared. The bypass capabilities of the RCIS permit clearing certain rod block conditions that are caused by failures or problems that exist in only one channel of the logic.

(8) RCIS Reliability

The RCIS has a high reliability and availability due to the total dual channel configuration in its design that allows its continual operation, when practicable, in the presence of component hardware failures. This is achieved by the operator being able to reconfigure the operation of the RCIS through bypass capabilities while the failures are being repaired.

The expected system availability during its 60-year life exceeds 0.99. The expected reliability is based upon the expected frequency of an inadvertent movement of more than one control rod. The expected frequency of an inadvertent movement of more than one control rod, due to failure, is less than or equal to once in 100 reactor operating years.

The RCIS design assures that no credible single failure or single operator error can cause or require a scram or require a plant shutdown. The RCIS design preferentially fails in a manner which results in no further normal rod movement.

(9) RCIS Bypass Capabilities

The RCIS provides the capability to bypass synchro A, if it is bad, and select synchro B for providing rod position data to both channels of the RCIS. The number and distribution of bypassed synchros are procedurally controlled by applicable plant Technical Specifications.

The RCIS allows the operator to completely bypass up to eight control rods by declaring them “Inoperable” and placing them in a bypass condition. Through operator action, an update in the status of the control rods placed into “inoperable” bypassed condition is available at the CRT display. At the display, the operator can request the data to be downloaded into the memory of the RAPI Subsystem logic with confirmation of a successful download completion signal being sent back to the CRT display.

Download of a new RCIS “Inoperable Bypass Status” to the RAPI Subsystem is only allowed when the RCIS is in a manual rod movement mode and when both keylock permissive switches are activated at the RCIS panels.

The operator can substitute a position for the rod that has been placed in a bypass state into both channels of the RCIS, if the substitute position feature is used. The substituted rod position value entered by the operator is used as the effective measured rod position that is stored in both rod action control channels and sent to other systems (e.g., the Process Computer System).

For purposes of conducting periodical inspections on FMCRD components, RCIS allows placing up to 21 control rods in “inoperable” bypass condition, only when the reactor mode switch is in REFUEL mode.

The RCIS enforces rod movement blocks when the control rod has been placed in an inoperative bypass status. This is accomplished by the RCIS logic by not sending any rod movement pulses to the FMCRD.

In response to activation of special insertion functions, such as ARI, control rods in bypass condition do not receive movement pulses.

(10) Single/Dual Rod Sequence Restriction Override (S/DRSRO) Bypass

The RCIS single/dual rod sequence restriction override bypass feature allows the operator to perform special dual or single rod scram time surveillance testing at any power level of the reactor. In order to perform this test, it is often necessary to perform single rod movements that are not allowed normally by the sequence restrictions of the RCIS.

When a control rod is placed in a S/DRSRO bypass condition, that control rod is no longer used in determining compliance to the RCIS sequence restrictions (e.g., the ganged withdrawal sequence and RRPS).

The operator can only perform manual rod movements of control rods in the S/DRSRO bypass condition. The logic of the RCIS allows this manual single/dual rod withdrawals for special scram time surveillance testing.

The operator can place up to two control rods associated with the same hydraulic control unit (HCU) in the S/DRSRO bypass condition.

The dedicated RCIS operator interface panel contains status indication of control rods in a S/DRSRO bypass condition.

The RCIS ensures that S/DRSRO bypass logic conditions have no effect on special insertion functions for an ARI or SCRAM following condition and also no effect on other rod block functions, such as MRBM, APRM, or SRNM period.

The drive insertion following a dual/single rod scram test occurs automatically. The operator makes the necessary adjustment of control rods in the system prior to the start of test for insertions, and restores the control rod to the desired positions after test completion.

The RCIS is a dual channel system and the logic of the system provides a capability for the operator to invoke bypass conditions that affect only one channel of the RCIS. The interlock logic prevents the operator from placing both channels in bypass. Logic enforces bypass conditions to ensure that the capability to perform any special function (such as an ARI, scram following, and SCRRI) is not prevented.

The RCIS logic ensures that any special restrictions that are placed on the plant operation are enforced as specified in the applicable plant Technical Specifications for invoked bypass conditions.

The status and extent of the bypass functions are identified on the RCIS dedicated operator interface panel and the PMCS CRT displays at the main control panel.

Bypass conditions allow continuation of normal rod movement capability by bypassing failed equipment in one RCIS channel. After repair or replacement of the failed equipment is completed, the operator can restore the system or subsystem to a full two-channel operability. The operator has the capability to invoke bypass conditions within the following system or subsystems:

(a) Synchro A or B position bypass

(b) Rod server module channel A or B bypass

(c) Inoperable condition bypass

(d) File control module channel A or B bypass

(e) ATLM channel A or B bypass

(f) RWM channel A or B bypass

(g) RACS channel A or B bypass

(11) Scram Time Test Data Recording

The logic of the RCIS provides the capability to automatically record individual FMCRD scram timing data based upon scram timing reed switches. When a FMCRD scram timing switch is activated, the time of actuation is recorded by the RAPI System for time tagging of stored scram time test data in the RSPC for that particular FMCRD. The time-tagged data is stored in memory until the next actuation of that particular reed switch is detected again.

The RCIS also time tags the receipt of a reactor scram condition being activated based upon the scram-following function input signals from the Reactor Protection System.

The resolution of this time-tagging feature is less than 5 milliseconds. Contact bounce of the reed switch inputs are properly masked to support this function. The reference real time clock for time tagging is the real time clock of the RCIS.

When the RCIS detects a reactor scram condition, the current positions of all control rods in the core are recorded, time tagged, and stored in memory. RCIS logic stores this data in memory until a request is received from the PMCS. The transmitted data is used by the PMCS to calculate and summarize

scram time performance based on the scram timing data received from the RCIS.

In an alternate design, the scram time recording and analysis functions are performed by two separate panels called scram time test panel (STTP) and scram time test recording/analysis panel (STR/AP). The STTP function is to directly interface with FMCRD reed switches and gather all FMCRD status and scram information. The function of STR/AP is to receive FMCRD information from STTP, process and analyze FMCRD scram time data, generate scram time test reports, and communicate FMCRD reed-switch-based status data to other plant systems.

(12) ATLM Algorithm Description

The ATLM is a microprocessor based subsystem of the RCIS that executes two different algorithms for enforcing fuel operating thermal limits. One algorithm enforces operating limit minimum critical power ratio (OLMCPR), and the other the operating limit minimum linear heat generation rate (OLMLHGR). For the OLMCPR algorithm, the core is divided into 48 regions, each region consisting of 16 fuel bundles. For the OLMLHGR algorithm, each region is further vertically divided up into four segments. During a calculation cycle of ATL (about 100 msec), rod block setpoints (RBS) are calculated for OLMCP monitoring (48 values) and for OLMLHGR monitoring (48 x 4 values). Then the calculated setpoints are compared with the real time averaged LPRM readings for each region/segment. The ATLM issues a trip signal if any regionally averaged LPRM reading exceeds the calculated RBS. This trip signal causes a rod block within the RCIS and also a flow change block in the Recirculation Flow Control System (RFCS).

Provided below is a summary description of OLMCPR and OLMLHGR RBS calculation methodology.

(a) **OLMCPR RBS Calculation Methodology**. The 16 fuel bundles of each region are surrounded by four LPRM strings. There are four LPRMs in each string. For regional OLMCPR monitoring, the sum of the average of each level of B, C, and D of the four LPRM strings is used. The formula for calculating the OLMCPR RBS is:

$$RBS_o = \frac{LPRM_i * A_o * RMCPR_1}{OLMCPR} \qquad (7.7\text{-}1)$$

where:

$RBS_o$ = Operating limit rod block setpoint.

$LPRM_i$ = Initial sum of average of four LPRMs of B, C, and D levels that surround each region.

$A_o$ = Margin factor for operating limit rod block; a known function of rod pull distance.

$RMCPR_i$ = Regional initial MCPR (i.e., the minimum CPR of the 16 bundles in the region spanned by the four LPRM strings). Known input from predictor (process computer).

OLMCPR = Operating limit MCPR in the current cycle; a known function of power.

Equation 7.7-1 is applicable to cases where there is no core flow change and when only one control rod is moved. Adjustments are made to the calculated $RBS_o$ to account for changes in core flow and adjacent control rods movements.

(b) **OLMLHGR RBS Calculation Methodology**. The formula for calculating the OLMLHGR RBS is:

$$RBS_m(X) = \frac{LPRM_i(X) * B_m * M_p}{MAPRAT_i(X)} \qquad (7.7\text{-}2)$$

where:

$RBS_m(X)$ = Calculated operating limit maximum average planar linear heat generation rate (OLMAPLHGR) RBS at LPRM level X.

$LPRM_i(X)$ = Initial average of the four LPRMs (level X) at the four corners of each 16-bundle fuel region. The region monitored by the level LPRM is the region covered up to .46m above and below the LPRM (0.914m total).

B(X) = Margin factor for MAPLH GR operating limit rod block for X level LPRMs. A known function of power and rod position.

$M_p$ = Off-rated power factor to consider overpower condition during worst transient at off-rated condition. A known function of power.

$MAPRAT_i(X)$ = Regional initial maximum MAPRAT for level X (i.e., the maximum MAPRAT of the 16 bundles within the 0.914m section covered by the X level LPRMs). A known input from 3D monitor.

In Equations 7.7-1 and 7.7-2 above, "initial" refers to values that are downloaded from the "3D Predictor Monitor" subsystem of the PMCS. A download is requested by the ATLM whenever changes in reactor power and/or core flow exceed a preset limit. A download can also be manually requested by the operator.

#### 7.7.1.2.2 System Interfaces

(1) Control Rod Drive (CRD) System

The RCIS interfaces with the CRD System are as follows:

(a) Synchros A and B of each FMCRD

(b) Coupling check (overtravel-out) position reed switch of each FMCRD

(c) Latched Full-In and Full-In position reed switches of each FMCRD

(d) Scram Timing position reed switches which include reed switches at 0%, 10%, 40%, 60%, +100% rod insertion for each FMCRD

(e) Separation reed switches (A&B) through the plant essential multiplexing system for each FMCRD

(f) "LOW CRD CHARGING WATER HEADER PRESSURE" condition (four signals to each channel of RCIS)

(g) Electrical power connections from RCIS to FMCRD motor, brake, and valve 143

(2) Recirculation Flow Control System (RFCS)

(a) Alternate Rod Insertion (ATWS) (Anticipated Transient Without Scram)

The RCIS logic (during an ATWS), on receipt of ARI signals from the RFCS, initiates the RCIS ARI function which controls the FMCRD motors such that all control rods are driven to their full-in position automatically. The three channels of the RFCS provide each of the two channels of the RCIS logic with the ARI signal. RCIS internal logic to initiate the RCIS ARI function is based on two-out-of-three logic within each channel of the RCIS. The operator, at the RCIS dedicated operator interface, can take action and initiate the ARI function. Two manual actions are required to manually initiate ARI.

The logic of the RCIS is designed such that no single failure results in failure to insert more than one operable control rod when the ARI function is activated.

(b) Selected Control Rod Run In (SCRRI) and Rod Block Functions

The three channels of the Recirculation Flow Control System (RFCS) provide each of the two channels of the RCIS with the separate isolated trip signals indicating the need for rod block automatic selected control rod run-in. The operator, at the RCIS dedicated operator interface, can also take action and initiate the SCRRI function. Two manual actions are required to manually initiate SCRRI.

The automatic SCRRI can either be initiated from the Feedwater Control System (FWCS) of the RFCS. The initiating event for the FWCS to generate a SCRRI signal is loss of feedwater heating (for detailed description of SCRRI initiation by FWCS, see Subsection 7.7.1.4). Each channel of the FWCS provides three signals to three channels of the RFCS. Each RFCS channel, after a two-out-of-three voting of these signals, generates a RFCS SCRRI signal which is sent to both channels of RCIS.

When two or more RIPs are tripped, the trip signal is "ANDED" with the reactor power level and core flow signals. If core flow is < 36% of rated and rated reactor power level is > 25% but less than 30%, the RFCS issues a rod block signal. In the same manner, if reactor power is ≥30%, the RFCS issues the SCRRI signal.

The RFCS receives reference power level signals from the Neutron Monitoring System and compares the reference power level signals with the nominal power level setpoint.

The RFCS rod block or SCRRI function is bypassed when power level is below the applicable specified setpoints, or when the core flow is above the specified setpoint.

The SCRRI function is not a safety-related function. The function is designed to meet the reliability requirement that no single failure shall cause the loss of SCRRI function.

The RFCS automatic initiation signal for the rod block/SCRRI function is sent as two independent sets of signals, two sets of three signals to each channel of RCIS. After two-out-of-three voting within each channel, depending on the signals received, the RCIS either issues a rod block signal and/or uses the FMCRD stepping motors of preselected control rods to drive them to their target SCRRI positions. Either channel of RCIS is capable of initiating the rod block/SCRRI functions on receipt of the signals from the RFCS.

The preselected control rods for a SCRRI function are selected at the RCIS CRT displays of the performance monitoring and control system in the main control room. The preselected SCRRI rod data are stored in memory in the RAPI Subsystem of the RCIS. The total control rod worth for the preselected control rods is designed to bring down the reactor power rod line from the 100% power rod line to the 80% power rod line.

The RCIS dedicated operation interface also provides control switches that require two manual operator actions for the operator to manually initiate the SCRRI function.

For manual or automatic initiation of the SCRRI function, the RCIS dedicated operator interface provides status indications and alarm annunciators in the control room.

The total delay time from the recirculation pump trip to the start of control rod motion, for the preselected control rods, is less than or equal to 2 seconds.

(c) RFCS Core Flow Signal to RCIS

The RFCS provides signals to both channels of the RCIS that represent validated total core flow. These signals are used for part of the validity checks when performing an ATLM operating limit setpoint update. The RCIS obtains these signals from the RFCS via the multiplexing system links to the RCIS channels.

(d) RCIS Signals to RFCS

The ATLM Subsystem of the RCIS issues a Flow Increase Block signal to RFCS whenever there is an ATLM trip.

The RCIS MUX Monitor provides hard-wired run-back signals to adjustable speed drives of the RFCS.

(e) RFCS Hard-Wired Signals to RCIS

Each of the three channels of RFCS provides the status of six relay contacts (12 wires per RFCS channel) to the RCIS. These signals are used by RCIS logic to minimize the likelihood inadvertent FMCRD run-in.

(3) Feedwater Control System (FWCS)

The Feedwater Control System provides signals to both channels of the logic of the RCIS that represents validated total feedwater flow to the vessel and

validated feedwater temperature. These signals are used as part of the validity checks when performing an ATLM operating limit setpoint update.

The RCIS can obtain these signals from the FWCS via the multiplexing system communication links to the RCIS channels.

(4) Neutron Monitoring System

Each of the four divisions of the Neutron Monitoring System provides independent signals to both channels of the RCIS that indicate when the following conditions are active:

(a) Startup range neutron monitor (SRNM) period alarm

(b) SRNM downscale alarm

(c) SRNM upscale alarm

(d) Average power range monitor (APRM) upscale alarm

(e) SRNM inoperative

(f) APRM downscale

(g) Flow-biased APRM rod block

(h) APRM inoperative

(i) Period-based rod withdrawal permissive

(j) Flow upscale alarm

Whether or not some of the signals result in a rod block depends on reactor mode switch status which is provided to the RCIS from the reactor protection system via the essential multiplexing system.

Each of the four divisions of NMS provides APRM, LPRM and core flow signals to the two channels of logic in the RAPI Subsystem for determining whether reactor power is above or below the low power setpoint and usage by ATLM.

The four divisions of the NMS provide the same signals to both channels of the RCIS. These signals meet the isolation and separation requirements of interfacing the Class 1E NMS with the non-Class 1E RCIS.

Each of the two MRBM non-safety subsystems of the NMS provide their rod block signals to the RCIS. The RCIS, in return, provides ATLM status signals and coordinates of the selected rods to MRBM.

(5) Reactor Protection System

Each of the four divisions of the RPS provides the RCIS two-channel system with separate isolated signals for indication of the reactor mode switch positions: SHUTDOWN, REFUEL, STARTUP and RUN.

The four divisions of the Reactor Protection System (RPS) each provide RCIS with two separate isolated signals for the low charging water header pressure trip switches in bypass position.

The Essential Multiplexing System provides the above signals to the RCIS with complete isolation between the safety-related system and the non-safety-related system equipment.

Divisions II and III of the RPS each provide the two channels of RCIS with two separate isolated signals that indicate a scram condition. The signals remain active until the scram condition is cleared by the operator. In addition, Divisions II and III of RPS each provide the RCIS with hard-wired relay contact status to minimize the likelihood of inadvertent FMCRD run-in.

(6) Performance Monitoring and Control System

The PMCS provides the data update from the 3-D predictor function calculations associated with ATLM parameters based on actual measured values from the plant. This data is downloaded into the ATLM memory. This is to assure that rod blocks occur if the operating limits (e.g., MCPR and MLHGR) are approached. This feature allows the ATLM rod block setpoint calculation to be based on actual, measured plant conditions.

The RCIS provides the PMCS with control rod position information along with other RCIS status information for use in other PMCS functions and for the PMCS CRT displays related to the RCIS.

The RCIS gathers, time tags, stores, and transmits scram timing data to the PMCS. The PMCS utilizes rod scram timing data to evaluate scram performance of the CRD System. The PMCS provides for the capability of printing or displaying of scram time logs. The scram time data sent to the PMCS provides the capability for comparing received data from the RCIS with the specification for control rod scram timing. Included in these comparisons are the averages and trends for data collected from past rod scrams or rod testing. The output for this function consists of, but is not limited to, the following type of data:

(a) Scram time measurements of any selected rod or group of rods to a particular position.

(b) A listing of INOPERABLE rods.

(c) Statistical analysis and average calculations of insertion times.

(d) List of rods which do not meet technical specification requirements.

In the alternate design, scram time recording and analysis functions are performed by separate panels.

(7) Automatic Power Regulator (APR) System

The APR System provides the automatic control rod movement commands to the two channels of the RCIS when the APR System and RCIS are in the automatic mode. The APR System includes the supervisory control logic for determining when to insert, withdraw, or stop control rods. The RCIS then determines which rods to move, based of the RRPS and current rods positions. The APR System is described in Subsection 7.7.1.7.

#### 7.7.1.2.3 Reactor Operator Information

(1) The RCIS provides for the activation of the following annunciation at the main control panel.

(a) Rod withdrawal blocks.

(b) Rod Control & Information System trouble.

(c) Low power transient zone (i.e., reactor power above but nearing the LPSP).

(d) Gang misalignment.

(e) Selected control rod run-in (SCRRI).

(f) Alternate rod insertion initiated.

(g) CRD charging water header pressure low.

(h) Reference rod pull sequence (RRPS) violation.

(i) ATLM trouble.

(2) The RCIS provides status information indication on the RCIS dedicated operators interface on the main control panel as follows:

(a) Whether RCIS rod movement mode is automatic or manual.

(b) Number of FMCRDs in their full-in position.

(c) Number of FMCRDs in latched full-in position.

(d) Number of FMCRDs in full-out position.

(e) Average percent insertion of all FMCRDs.

(f) Identification of selected gang (or selected single rod).

(g) Average percent insertion of selected gang (or selected single rod).

(h) Number of FMCRDs in an inoperable bypass condition.

(i) Existence of any rods withdrawal blocks.

(j) Existence of any single channel bypass of the RACCS and/or any subsystem within the RACCS.

(k) Whether reactor power is above the LPSP.

(l) Existence of RCIS trouble.

(m) Activation of scram following function.

(n) Activation of the ARI function.

(o) Status of SCRRI function.

(p) Successful completion of ATLM operating limit setpoint update.

(q) Any control rod in S/DRSRO bypass condition.

(r) Activation of a rod block by MRBM condition.

(3) The dedicated operators interface panel of the RCIS provides logic and operator controls, so that the operator can perform the following functions:

(a) Change the RCIS mode of operation from manual to semi-automatic or automatic rod movement modes.

(b) Manually initiate the SCRRI function.

(c) Manually initiate the two CRD test functions.

(d) Request a bypass of RACCS channel A or B (normal position: no bypass).

(e) Request a bypass of ATLM or RWM channel A or B. (Normal positions are not bypassed.)

(f) Request an ATLM operating limit setpoint update be performed.

(g) Perform a reset of any RCIS.

(h) Manually initiate CRD brake test, CRD coupling check and CRD step test functions.

NOTE: Interlock logic may prevent certain combinations of bypasses from being activated even though the above bypass controls have been activated.

(4) The CRT displays, which are part of the PMCS, provide information to the operator on demand.

The following status and controls are available through the CRTs:

(a) RCIS rod movement status (automatic/semi-automatic/manual).

(b) Position of all rods, based on synchro signals.

(c) Selected gang (or selected single rod) plus the four LPRM readings of the closest LPRM strings to the selected gang or selected single rod. If the closest LPRM reading at a given level is inoperable, as determined by the Neutron Monitoring System LPRM status information, an INOP status is displayed instead of actual LPRM reading.

Identification of: (d through v)

(d) All rods in rod withdrawal block condition.

(e) BYPASSED or INOPERABLE control rods.

(f) Control rods with bypassed synchros.

(g) Control rods that separation has been detected.

(h) Control rods full-in status.

(i) Control rods in latched full-in status.

(j) Control rods in overtravel-out status.

(k) Control rods full-out status.

(l) Control rods in overtravel-out status.

(m) Control rods for which uncoupled condition has been detected.

(n) Control rods for which drift condition has been detected.

(o) Control rods for which abnormal movement (other than drift) has been detected.

(p) Control rods that are SCRRI selected control rods.

(q) Control rods that can be inserted.

(r) Control rods that can be withdrawn.

(s) All RCIS bypasses in effect.

(t) All detected conditions that have resulted in an RCIS trouble alarm being activated, when applicable.

(u) All detected conditions that have resulted in rod withdrawal block conditions being active, when applicable.

(v) Obtain ATLM operating limit setpoint update, when requested.

#### 7.7.1.2.4 Test and Maintenance

The RCIS equipment is designed with online testing capabilities. The system can be maintained on line while repairs or replacement of hardware take place without causing any abnormal upset condition.

The system has been designed so that removal or repair of modules or cards can be performed without the use of special tools.

#### 7.7.1.2.5 Environmental Considerations

The RCIS equipment is qualified by tests or analysis to meet the environmental conditions in Section 3.11. The equipment that is located within the control room is qualified to control room requirements.

The RCIS hardware has been designed for a 60 year design life and systematic wearout failures were considered in determination of the design life. Random failures were considered in calculating the system availability and reliability.

### 7.7.1.3 Recirculation Flow Control System—Instrumentation and Controls

(1) Identification

The objective of the Recirculation Flow Control (RFC) System is to control reactor power level, over a limited range, by controlling the flow rate of the reactor core water.

The RFC System consists of three redundant process controllers, adjustable speed drives (ASDs), switches, sensors, and alarm devices provided for operational manipulation of the ten reactor internal pumps (RIPs) and the surveillance of associated equipment. Recirculation flow control is achieved either by manual operation or by automatic operation if the power level is above 70% of rated. The reactor internal pumps can be driven to operate anywhere between 30% to 100% of rated speed with the variable voltage, variable frequency power source supplied by the ASDs. 30% rated speed corresponds to the minimum operating speed to be used during initial pump startups. The instrument electrical diagram (IED) is provided in Figure 7.7-5 and the interlock block diagram (IBD) is provided in Figure 7.7-7.

(2) Classification

This system is a power generation system and is classified as not required for safety.

(3) Power Sources

(a) Normal

Each processing channel of the triply redundant digital processor receives its respective power input from an uninterruptible, independent source of the instrument and control power supply system. Other system equipments such as the transmitters, input conditioners, voters, output device drivers, control room displays, etc., will also derive their required power sources from the same redundant uninterruptible power supply system.

Variable voltage, variable frequency electrical power is generated by the adjustable speed drives (ASDs) for use by the induction motors in the RIPs. Four medium voltage power buses are used to provide input power to the ten ASDs. These buses are fed from the unit auxiliary transformers connecting to the main turbine-generator. Two of the buses each provide power directly to a pair of ASDs. The other two buses each provide power to a motor-generator (M-G) set which, in turn, supplies power to three ASDs operating in parallel (see one-line diagram for AC power distribution provided as Figure 8.3-2).

The allocation of the RIP equipment on the four power buses is such that on loss of any single power bus, a maximum of three RIPs are affected. At least one circuit breaker is provided along each circuit path to protect power equipment from being damaged by overcurrent.

(b) Alternate and Startup

During the plant startup, or on loss of normal auxiliary power, reserve auxiliary transformer provides backup power to the medium voltage normal auxiliary power systems. The M-G set flywheels provide sufficient inertia for six of the RIPs to extend core flow coastdown time, thereby reducing the change in MCPR during the momentary voltage drop transient.

(4) Normal Operation

Reactor recirculation flow is varied by modulating the recirculation internal pump speeds through the voltage and frequency modulation of the adjustable speed drive output. By properly controlling the operating speed of the RIPs, the recirculation system can automatically change the reactor power level.

Control of core flow is such that, at various control rod patterns, different power level changes can be automatically accommodated. For a rod pattern where rated power accompanies 100% flow, power can be reduced to 70% of full power by full automatic or manual flow variation. At other rod patterns, automatic or manual power control is possible over a range of approximately 30% from the maximum operating power level for that rod pattern. Below 70% power level, only manual control of power (i.e., by means of manual flow setpoint control) is available.

An increase in recirculation flow temporarily reduces the void content of the moderator by increasing the flow of coolant through the core. The additional neutron moderation increases reactivity of the core, which causes reactor power level to increase. The increased steam generation rate increases the steam volume in the core with a consequent negative reactivity effect, and a new (higher) steady-state power level is established. When recirculation flow is reduced, the power level is reduced in the reverse manner. The RFC System, operating in conjunction with the main turbine pressure regulator control, provides fully automatic load following.

The RFC System is designed to allow both automatic and manual operation. In the automatic mode, either total automatic or semi-automatic operation is possible. Fully automatic, called “Master Auto” mode, refers to the automatic load following (ALF) operation in which the master controller receives a load demand error signal from the main turbine pressure regulator. The load demand error signal is then applied to a cascade of lead/lag and proportional-integral (PI) dynamic elements in the master controller to generate a flow demand signal for balancing out the load demand error to zero. The flow demand signal is forwarded to the flow controller for comparing with the sensed core flow. The resulting flow demand error is used to generate a suitable gang speed demand to the ASDs. The speed demand to the individual ASDs causes adjustment of RIP motor power input, which changes the operating speed of the RIP and, hence, core flow and core power. This process continues until both the errors existing at the input of the flow controller and master controller are driven to zero. Fully automatic control is provided by the master controller when in the automatic mode. The flow controller can remain in automatic even though the master controller is in manual.

The reactor power change resulting from the change in recirculation flow causes the pressure regulator to reposition the turbine control valves. If the original demand signal was a load/speed error signal, the turbine responds to the change in reactor power level by adjusting the control valves, and hence its power output, until the load/speed error signal is reduced to zero.

In the semi-automatic mode, the operator sets the total core flow demand and the RFC System responds to maintain a constant core flow. Core flow control is achieved by comparing the core flow feedback, which is calculated from the core plate differential pressure signals, with the operator-supplied core flow setpoint.

In total manual control, the operator can directly manipulate the pump speeds. Pump speeds can be controlled individually or collectively. When individually controlled, pump speed demand is obtained through the operator console and transmitted directly to the individual adjustable speed drive (ASD) for pump frequency control. In collective manual operation, a common speed setpoint is used for controlling each RIP which has been placed in the GANG speed control mode.

(5) Startup Operations

The RFC System is also used to control the startup of the reactor internal pumps. To minimize thermal shock to the reactor vessel, the RFC System will prevent startup of an idle RIP if the temperature of the vessel bottom coolant is not within 80°C of the saturated water temperature corresponding to the steam dome pressure. The vessel bottom temperature, supplied by the Reactor Water Cleanup (CUW) System, is compared with the saturated water temperature derived from the wide range dome pressure signal, to determine the actual temperature difference.

Startup of the RFC System begins by sequentially bringing each RIP up to the minimum operating limit (30% of rated speed). It is not permitted to raise a particular pump's speed above the minimum limit until all desired pumps have started and reached the minimum speed. This restriction is imposed to avoid overdriving the ASDs against an excessive starting load which can be developed by the higher pump speed/head.

(6) Abnormal Conditions

The RFC System provides logic to initiate actions which can mitigate the effect of certain expected operational transients. These include RIP speed runbacks to some decreased flow conditions, pump trips (RPTs), or commands to the

RCIS demanding rod motion block or rod insertion for stability and protection control. These trip functions are shown in Figure 7.7-7

(7) Recirculation Pump Trip (RPT)

In the event of either (a) turbine trip or generator load rejection when reactor power is above a predetermined level (EOC RPT), (b) reactor pressure exceeds the high dome pressure trip setpoint, or (c) reactor water level drops below the Level 3 setpoint, the RPT logic will automatically trip off a group of four RIPs. The group of the RIPs being tripped is the same group which derives its power source directly from the 6.9 kV buses (i.e., the group not having the M-G set interface).

The three inputs required to determine the preceding three RPT conditions are provided by the Reactor Protection System, the Feedwater Control System, and the Steam Bypass and Pressure Control System. These inputs consist of three sets of discrete signals for each of the end-of-cycle (EOC), high pressure and low level (Level 3) trip conditions. Each set represents the status of four channel outputs. A two-out-of-four logic is used by the RFC System to confirm the validity of the EOC trip condition. Two-out-of-three logic is used for the high pressure and Level 3 trip conditions. Any one of the three trip conditions can initiate a RPT. All switching logics are performed by the triplicate RFC controller. RPT is implemented by tripping the gate-turn-off (GTO) inverters in the adjustable speed drives.

After tripping off the first group of four RIPs, if reactor water level continues to drop and reaches Level 2, the remaining six RIPs will be tripped, three immediately and the final three after a preset time delay. The implementation of the second RPT function is similar to the EOC RPT, using two-out-of-four confirmation logic. The level 2 trip signal is provided by the Nuclear Boiler System. All RPT functions are non-safety-related.

(8) Equipments

(a) Reactor Internal Pumps (RIPs)

The Reactor Recirculation System incorporates 10 RIPs with their impellers and diffusers internal to the reactor vessel. The RIPs themselves are mounted vertically onto and through the pump nozzles that are arranged in an equally-spaced ring pattern on the bottom head of the reactor pressure vessel. The RIPs are single stage, vertical pumps driven by variable speed induction motors. The pump speed is changable by varying the voltage and frequency output of the individual pump motor electrical power supply.

The RIPs provide recirculation flow through the lower plenum and up through the lower grid, the reactor core, steam separators, and downcomers. The flow rate is variable over a range from minimum flow established by the pump characteristics to above the maximum flow required to obtain rated reactor power.

(b) RIP Motors

The RIP motors are the variable speed, four-pole, AC induction wet motor type. The operating speed of the pump motor depends on the variable-voltage / variable-frequency output of the ASDs. The RIP motors are cooled by water from the primary side of the reactor motor heat exchangers (RMHXs). Heat in the secondary side of the heat exchanger is removed by the Reactor Building Cooling Water System. There is one heat exchanger per motor.

A clean purge flow is provided by the Control Rod Drive System to inhibit reactor water from entering the motor cavity region, thereby preventing any impurity buildup. Also, anti-reverse rotation devices are installed on the motor shaft to prevent possible motor damage due to reverse pump flow.

(c) Adjustable Speed Drives (ASDs)

ASDs are used to provide electrical power and speed control to the pump motors in the RIPs. Each ASD receives electrical power at a constant AC voltage and frequency. The ASD converts this to a variable frequency and voltage in accordance with the speed demand requested by the RFC System controller. The variable frequency and voltage is supplied to vary the operating speed of the recirculation pump motor.

Each ASD consists of (1) an AC-to-DC rectifier section; (2) a solid state, variable frequency DC-to-AC inverter section, which includes gate-turn-off thyristers for implementation of the RPT function; (3) a control and regulation section; and (4) measurement and protection circuits.

The ASD is capable of supporting three modes of operation: startup, normal and shutdown. When the startup mode is selected, the invertor output quickly steps up from zero to the required motor power corresponding to the minimum pump speed to 30%, and holds at that output frequency. When the normal operation mode is selected, continuous output power frequency between 30% and 100% is allowed. The operation of the shutdown mode is exactly reverse that of the normal and startup mode; ASD output is automatically ramped to 30% frequency, then stepped down to zero.

(d) Fault-Tolerant Digital Controller

The RFC System control functional logic is performed by a triply redundant, microprocessor-based fault-tolerant digital controller (FTDC). The FTDC consists of three identical processing channels working in parallel to provide fault-tolerant operation.

The FTDC performs many functions. It reads and validates inputs off the Non-Essential Multiplexing System (NEMS) interface once every sampling period. It performs the specific recirculation flow control calculations and processes the pertinent alarm and interlock functions, then updates all RFC System outputs to the NEMS. To prevent computational divergence among the three processing channels, each channel performs a comparison check of its calculated results with the other two redundant channels.

The internal FTDC architecture features three multiplexing (MUX) interfacing units for communication between the NEMS and the FTDC processing channels, and fiber optic communication links for interprocessor and channel communication, and for communication with the technician interface unit (TIU).

(e) Recirculation Flow Control System Algorithms

The RFC System design consists of two main control loops: (1) the core flow loop, which modulates pump speed demand to provide the desired core flow rate, and (2) the automatic load following (ALF) which modulates the core flow demand in response to the demands of the grid. In addition, pump speed in each RIP can be manually controlled individually or collectively. The RFC System algorithm structure is illustrated in Figure 7.7-5 (sheet 2).

In the core flow control mode, sensed core flow calculated by the core plate differential pressure method is compared with the core flow demand supplied by the operator or obtained from the master controller, depending on the RFC System operating mode. This flow error is passed through a flow error limiter, then input to the core flow proportional-integral (PI) controller to drive pump speed demand.

A function generator converts the speed demand output to frequency demand for the ASDs. A rate limiter on the output of the function generator limits the rate of change in speed demand to 1.5%/s for increasing speed changes and 5%/s for decreasing speed changes during normal operation. This prevents rapid changes in pump speed as a result of multiple processing channel failure.

In the ALF mode, the master controller receives a load demand signal from the Steam Bypass and Pressure Control (SB&PC) System in response to any combination of local operator load setpoint inputs, automatic generation control inputs, or grid load changes indicated by grid frequency variation.

The master controller functionally provides (1) a function generator which schedules a gain adjustment in accordance with the size of the load demand error, (2) a lead/lag compensator which improves steam flow response by means of zero/pole modification, and (3) a P-I controller which acts on the load demand error signal to balance the turbine outputs with the load demand.

All calculations required to support the control system algorithms, as well as the trip protective functions, are performed in parallel by three processing channels of the FTDC.

(f) Fault-Tolerant Voters

For each discrete and analog RFC System output, fault tolerance objective is achieved by performing a two-out-of-three vote on the three FTDC channel outputs.

For the critical RFC System outputs, such as the final processor output on the RIP speed demand, voter failure logic is provided to monitor the proper function of the speed demand voters. This is done by comparing the final speed demand with the demand ringback signals. Pump speed will lockup in the as-is condition if voter failure condition is detected. In addition, annunciation logic is provided to detect failures in the voter failure logic.

(g) Technician Interface Unit

A technician interface unit (TIU) allows the technician to perform troubleshooting, change control and calibration parameters in the FTDC, and to inject test signals into the control process for system testing. The TIU is implemented in a menu-driven format; it is designed such that its operation will not disturb the FTDC except when instructed by specific keyword commands. The use of passwords and/or keylock switches is required for certain commands which may result in modification of system parameters. The TIU also provides an information mode which allows the technician to examine process data, control configuration and processor status.

(h) Core Flow Measurement Systems

Two methods of core flow measurement are provided by the RFC System: (1) the core plate differential pressure (CPdP) method and (2) the pump deck differential pressure (PDdP) method.

With the CPdP method, the average differential pressure across the lower core support plate is measured by means of four equally-spaced pressure sensing transmitters. The coefficients used will be calibrated during startup against the results of the PDdP method.

Separate CPdP flow calculations are performed by both the RFC System and the NMS. Each system uses a separate set of pressure transmitters. The RFC CPdP flow results are used in the RFC process control. NMS flow results are used in safety function trips.

The PDdP measurement system consists of four differential pressure transmitters measuring the pump deck differential pressures common to all RIPs, and one set of redundant pump speed sensors unique for each RIP. Pump flows are calculated by the process computer based on information from the measured delta Ps, pump speed, and the vendor-supplied pump head curves. Total core flow is the sum of the individual pump flows. The PDdP core flow signal is used as a calibration source for CPdP core flow and as an input to the MCPR calculations.

(9) Testability

The FTDC, analog and discrete output voters, core flow measurement systems, ASDs and RIPs are continuously functioning during normal power operation. Any abnormal operation of these components can be detected during operation. In addition, the FTDC is equipped with self-test and online diagnostic capabilities for identifying and isolating failure of process sensors, I/O cards, buses, power supplies, processors, and interprocessor communication paths. These online tests and diagnosis are performed without disturbing the normal control functions of the RFC system.

(10) Environmental Considerations

The RFC System is not required for safety purposes, nor is it required to operate during or after any design basis accident. The system is required to operate in the normal plant environment for power generation purposes only.

The recirculation pump equipment is located in the lower drywell that is subjected to the environment under design conditions listed in Section 3.11.

The recirculation pump power supplies are located outside of the wetwell in the Reactor Building.

The logic, control unit and instrumentation terminals are located in the main control room and subject to the normal control room environment as listed in Section 3.11.

(11) Operational Considerations

The FTDC, which commands RIP speed changes, is located in the main control room. Provisions are made to allow either automatic or manual operation for each control loop (master, flow and speed). All transfers between the manual and automatic operations are designed to be bumpless. RFCS control modes, as well as setpoint changes, can be initiated by either the operator or by the PMCS, depending on whether the “local” or the “auto” system control has been selected.

When in local control, the operator’s control, panel provides the operator the capability to select the operating mode of the system and to initiate certain manual actions, and to increment / decrement switches which adjust setpoints at a preset rate of change.

(12) Reactor Operator Information

Indications and alarm are provided to keep the operator informed of the system operational modes and equipment status, thereby allowing him to quickly determine the origin of any abnormal conditions.

Control room indications include both dedicated displays and on-demand displays from the Process Monitoring and Control System. These indications include the digital recirculation flow controller process variables, the recirculation pump speed and POWER SUPPLY operating status, and the core flow measurement system outputs. Also, indicating lights are provided to indicate the control system configuration and the trip function status.

Alarms are provided to alert the control room operator of any malfunction in the processor inputs, RIPS, adjustable speed drives or the pump motor cooling systems, and automatic trips of protective functions.

(13) Setpoints

The subject system has no safety setpoints.

### 7.7.1.4 Feedwater Control System—Instrumentation and Controls

(1) System identification

The Feedwater Control System (FWCS) controls the flow of feedwater into the reactor pressure vessel to maintain the water level in the vessel within predetermined limits during all plant operating modes. The range of water level is based upon the requirements of the steam separators (this includes limiting carryover, which affects turbine performance, and carryunder, which affects reactor internal pump operation).

The FWCS may operate in either single or three-element control modes. At feedwater and steam flow rates below 25% of rated (when steam flow is either negligible or else measurement is below scale), the FWCS utilizes only water level measurement in the single-element control mode. When steam flow is negligible, the Reactor Water Cleanup (CUW) System dump valve flow can be controlled by the FWCS in single-element mode in order to counter the effects of density changes during heatup and purge flows into the reactor. At higher flow rates, the FWCS in three-element control mode uses water level, main steamline flow, main feedwater line flow, and feedpump suction flow measurements for water level control. The FWCS control structure is shown in the IED control algorithm detail in Figure 7.7-8. The interlock block diagram (IBD) is provided in Figure 7.7-9.

(2) Classification

The FWCS is a power generation (control) system with operation range between high water level (L8) and low water level (L2) trip setpoints. It is classified as non-safety-related.

(3) Power Sources

The triply redundant FWCS digital controllers and process measurement equipment is powered by non-Class 1E redundant uninterruptible power supplies (UPS). No single power failure shall result in the loss of any FWCS function.

(4) Equipment

The Feed Water Control System consists of the following elements:

(a) Triplicated Fault Tolerant Digital Controllers (FTDCs) located in the Control Building, which contain the software and processors for execution of the control algorithms.

(b) Feedwater flow transmitters, which provide the total flow rate of feedwater into the vessel.

(c) Steam flow transmitters, which provide the total flow rate of steam leaving the vessel.

(d) Feedpump suction flow transmitters, which provide the suction flow rate of each feedpump.

(e) The low flow control valve differential pressure transmitter, which provides the pressure drop across the low flow control valve.

(f) Adjustable speed drives (ASD) for the reactor feedwater pump (RFP).

(5) Reactor Vessel Water Level Measurement

Reactor vessel narrow range water level is measured by three identical, independent sensing systems which are a part of the Nuclear Boiler System (NBS). For each level measurement channel, a differential pressure transmitter senses the difference between the pressure caused by a constant reference column of water and the pressure caused by the variable height of water in the reactor vessel. The differential pressure transmitter is installed on lines which are part of the Nuclear Boiler System (Subsection 7.7.1.1). The FWCS FTDCs will determine one validated narrow range level signal using the three level measurements, received from NBS via the Non-Essential Multiplexing System (NEMS), as inputs to a signal validation algorithm. The validated narrow range water level is indicated on the main control panel and continuously recorded in the main control room.

(6) Steam Flow Measurement

The steam flow in each of four main steamlines is sensed at the reactor pressure vessel nozzle venturis. Two transmitters per steamline sense the venturi differential pressure and send these signals to the FTDCs via the NEMS. The NEMS signal conditioning algorithms take the square root of the venturi differential pressures and provide steam flow rate signals to the FTDCs for validation into one steam flow measurement per line. These validated measurements are summed in the FTDCs to give the total steam flow rate out of the vessel. The total steam flow rate is indicated on the main control panel and recorded in the main control room.

(7) Feedwater Flow Measurement

Feedwater flow is sensed at a single flow element in each of the two feedwater lines. Two transmitters per feedwater line sense the differential pressure and send these signals to the FTDCs via the NEMS. The NEMS signal conditioning

algorithms take the square root of the differential pressure and provide feedwater flow rate signals to the FTDCs for validation into one feedwater flow measurement per line. These validated measurements are summed in the FTDCs to give the total feedwater flow rate into the vessel. The total feedwater flow rate is indicated on the main control panel and recorded in the main control room.

Feedpump suction flow is sensed at a single flow element upstream of each feedpump. The suction line flow element differential pressure is sensed by a single transmitter and sent to the FTDCs via the NEMS. The NEMS signal conditioning algorithms take the square root of the differential pressure and provide the suction flow rate measurements to the FTDCs. The feedpump suction flow rate is compared to the demand flow for that pump, and the resulting error is used to adjust the actuator in the direction necessary to reduce that error. Feedpump speed change via adjustable speed drives and low flow control valve position control are the flow adjustment techniques involved.

(8) Feedwater/Level Control

Three modes of feedwater flow control, and thus level control, are provided which are selectable from the main control room.

— Single-element control

— Three-element control

— Manual control

Each FTDC will execute the control software for all three of the control modes. Actuator demands from the triply redundant FTDCs will be sent over the NEMS to field voters which will determine a single demand to be sent to each actuator. Each feedpump speed or control valve demand may be controlled either automatically by the control algorithms in the FTDCs or else manually from the main control panel through the FTDCs.

Three-element automatic control is provided for normal operation. Three-element control utilizes water level, feedwater flow, steam flow, and feedpump flow signals to determine the feedpump demands. The total feedwater flow is subtracted from the total steam flow signal yielding the vessel flow mismatch. The flow mismatch summed with the conditioned level error from the master level controller (proportional + integral) provides the demand for the master flow controller. The master flow controller output provides the demand for the feedpump flow loops, which send either a pump speed demand signal or

flow control valve signal through a linearizing function generator and then to the feedpump flow control actuator.

In the single-element control mode, which is employed at lower feedwater flow rates, only a conditioned level error is used to determine the feedpump demand. The master level controller (proportional + integral) conditions the level error and sends it directly to the feedpump actuator linearizing function generator and then to the feedpump flow control actuator itself. When the reactor water inventory must be decreased, during very low steam flow rate conditions, the CUW System dump valve is controlled by the FWCS in single element control. Reactor water is dumped through the CUW System to the condenser.

Each feedpump flow control actuator can be controlled “manually” from the main control panel by selecting the manual mode for that feedpump. In manual mode, the operator may increase or decrease the demand that is sent directly to the linearizing function generator of the chosen feedpump flow control actuator.

(9) Interlocks

The level control system also provides interlocks and control functions to other systems. When the reactor water level reaches the Level 8 trip setpoint, the FWCS simultaneously annunciates a control room alarm, sends a trip signal to the Turbine Control System to trip the turbine generator, and sends trip signals to the Condensate, Feedwater and Condensate Air Extraction (CF&CAE) System to trip all feed pumps and to close the main feedwater discharge valves and feedpump bypass valves. This interlock is enacted to protect the turbine from damage from high moisture content in the steam caused by excessive carryover while preventing water level from rising any higher. This interlock also prevents overpressurization of the vessel by isolating the condensate pumps from the vessel.

Upon detection of a loss of feedwater heating, the FWCS will send a signal to the Recirculation Flow Control System which will signal the Rod Control and Information System (RCIS) for initiation of automatic selected control rod run-in (SCRRI). This is done to minimize reactivity transient resulting from introduction of cold feedwater in such an event.

As an Anticipated Transient Without Scram (ATWS) mitigation measure, the FWCS issues signals to runback feedwater flow upon receipt of an ATWS trip signal from the Safety System and Logic Control (SSLC) System.

The FWCS will send a signal to the main steamline condensate drain valves to open when steam flow rate is below 40% of rated flow. This also protects the turbine from damage caused by excessive moisture in the steam line.

The FWCS will send a Level 4 trip signal to the Recirculation Flow Control (RFC) System when reactor water level reaches this low level setpoint. The RFC System use this signal in determining the need for performing a recirculation runback when a feed pump trip occurs. The RFC runback will aid in avoiding a low water level scram by reducing the reactor steaming rate.

The FWCS will send a Level 3 trip signal to RFC System to trip four reactor internal pumps (RIPs).

(10) Feedwater Flow Control

Feedwater flow is delivered to the reactor vessel through a combination of three adjustable speed motor-driven feedpumps which are arranged in parallel. During planned operation, the feedpump speed demand signal from the FTDCs is sent to a field voter which sends a single demand signal to the feed pump speed control systems. Each adjustable speed drive can also be controlled by its manual/automatic transfer station which is part of the Feedwater and Condensate System. A low flow control valve (LFCV) is also provided in parallel to a common discharge line from the feedpumps. During low flow operation, the LFCV demand signal from the FTDCs are sent to a field voter which sends a single demand signal to the LFCV control system. The LFCV can also be controlled by the manual/automatic transfer station which is part of the feedwater and condensate system.

The feedpump flow control actuator demand outputs from the field voters are “rung back” to the FTDCs so that they may be compared with the FTDC demand outputs. If there is difference between the field voter outputs and the FTDC demand outputs, an actuator “lockup” signal is sent to the feedpump flow control actuators via a “lockup” voter and an annunciator is initiated in the control room. If the “lockup” voter receives a majority of redundant “lockup” input signals, the actuator demand will be kept “as is” until the “lockup” condition is resolved. The “lockup” voter output signal is also “rung back” to the FTDCs so that a “lockup” voter failure can be recognized and an annunciator sounded in the control room.

(11) Testability

The FTDC self-test and online diagnostic test features are capable of identifying and isolating failures of process sensors, I/O cards, buses, power supplies, processors and inter-processor communication paths. These features

can identify the presence of a fault and determine the location of the failure down to the module level.

The FWCS components and critical components of interfacing systems are tested to assure that specified performance requirements are satisfied. Preoperational testing of the FWCS is performed before fuel loading to assure that the system will function as designed and that stated system performance is within specified criteria. Startup testing is performed to assure that stated system performance is within specified criteria and that the system will operate properly with other reactor control systems to achieve specified objectives.

(12) Environmental Conditions

The FWCS is not required for safety purposes, nor is it required to operate after the design basis accident. This system is required to operate in the normal plant environment for power generation purposes only.

(13) Operational Consideration

The FTDCs are located in the main control room where, at the operator's discretion, the system can be operated either in manual or automatic.

Manual control of the individual feedpumps and the LFCV is available to the operator in the main control room via the feedwater and condensate system controls.

In the event of low water level due to loss of feedwater, the RPS will cause plant shutdown, and emergency core cooling will be initiated to prevent lowering of vessel water level below an acceptable level.

(14) Reactor Operator Information

Indicators and alarms, provided to keep the operator informed of the status of the system, are as noted in previous subsections.

(15) Setpoints

The FWCS has no safety setpoints.

### 7.7.1.5 Process Computer System (PCS)—Instrumentation and Controls

(1) System Identification

The PCS includes two subsystems, the Performance Monitoring and Control Subsystem (PMCS) and the Power Generation Control Subsystem (PGCS). Between them, the two subsystems perform the process monitoring and

control and the calculations that are necessary for the effective evaluation of normal and emergency power plant operation. The PCS is designed for high reliability utilizing redundant, network combined processing equipment which is capable of processing data, servicing subsystems, providing supervisory control over digital control systems and presenting data to the user.

The purpose of the PCS is to increase the efficiency of plant performance by:

(a) performing the functions and calculations defined as being necessary for the effective evaluation of nuclear power plant operation;

(b) providing the capability for supervisory control of the entire plant by supplying setpoint commands to independent non-safety-related automatic control systems as changing load demands and plant conditions dictate;

(c) providing a permanent record and historical perspective for plant operating activities and abnormal events;

(d) providing analysis, evaluation and recommendation capabilities for startup, normal operation, and plant shutdown;

(e) providing capability to monitor plant performance through presentation of video displays in the main control room and elsewhere throughout the plant; providing the ability to directly control certain non-safety-related plant equipment through on-screen technology; and

(f) providing an interface to the plant simulator for training and for development and analysis of operational techniques.

The calculations performed by the process computer include process validation and conversion, combination of points, nuclear system supply performance calculations, and balance-of-plant performance calculations.

(2) Classification

The Process Computer System (PCS) is classified as a non-safety-related system and has no safety-related design basis. However, it is designed so that the functional capabilities of safety-related systems are not affected by it.

(3) Power Sources

The power for the PCS is supplied from two vital ac power supplies. These are redundant, uninterruptible non-Class 1E 120 Vac power supplies. No single power failure will cause the loss of any PCS function.

(4) Equipment

The PCS is composed of the following features and components:

(a) The central processing units, which perform various calculations, make necessary interpretations and provide for general input/output device control between I/O devices and memory.

(b) An automatic prioritizing function that provides processor capability to respond immediately to important process functions and to operate at optimum speed.

(c) A random access type processor memory that has a memory parity check feature capable of stopping computer operation subsequent to completing an instruction in which a parity error is detected. The processor memory has suitable shutdown protection to prevent information destruction in the event of loss of power or incorrect operating voltage.

(d) The capability to maintain real time by utilizing necessary calendar-type programs to compute year, month, day, hour, minute, second and either cycles or milliseconds. This is done automatically except in the event of processor shutdown.

(e) Bulk memory for storing all programs and all data. Capability is provided to protect selectable portions of bulk memory against information destruction caused by an inadvertent attempt to write over the programs or by a system power failure.

(f) Peripheral I/O equipment that is used to read data into and out of the computer.

(g) Process I/O hardware that accepts both analog and digital inputs. Intermittent signals and pulse type inputs are sensed by automatic priority interrupt.

(h) Means to permit the operator to enter information into the computer and request various special functions during routine operation. Diagnostic alarms, displays and associated function selection switches permit the operator to communicate with the processors.

(i) Peripheral equipment in the computer room that is used by programmers and maintenance personnel to permit necessary control of the system for trouble shooting and maintenance functions.

(5) Testability

The PCS has self-checking provisions. It performs diagnostic checks to determine the operability of certain portions of the system hardware and performs internal programming checks to verify that input signals and selected program computations are either within specific limits or within reasonable bounds.

(6) Environmental Considerations

(See Subsection 3.8.4.3.2)

(7) NSS Performance Calculation Programs

The NSS programs provide the reactor core performance information. The functions performed are as follows:

(a) The local power density for every fuel assembly is calculated using plant inputs of pressure, temperature, flow, LPRM levels, control rod positions, and the calculated fuel exposure.

(b) Total core thermal power is calculated from a reactor heat balance. Iterative computational methods are used to establish a compatible relationship between the core coolant flow and core power distribution. The results are subsequently interpreted as power in specified axial segments for each fuel bundle in the core.

(c) After calculating the power distribution within the core, the computer uses appropriate reactor operating limit criteria to establish alarm trip settings (ATS) for each LPRM channel. These settings are expressed as maximum acceptable LPRM values to which the actual scanned LPRM readings are compared. The scanned LPRM, when exceeding the ATS, will sound an alarm and thereby assist the operator to maintain core operation within permissible thermal limits established by the prescribed maximum fuel rod power density and minimum critical power ratio criteria. LPRM calibration constants are periodically calculated.

(d) The core power distribution calculation sequence is completed periodically and on demand. Subsequent to executing the program, the computer prints a periodic log for record purposes. Key operating parameters are evaluated based on the power distribution and edited on the log.

(e) Each LPRM reading is scanned at an appropriate rate and, together with appropriate computational methods, provides nearly continuous

reevaluation of core thermal limits with subsequent modification to the LPRM ATS based on the new reactor operating level. The range of surveillance and the rapidity with which the computer responds to the reactor changes permit more rapid power maneuvering with the assurance that thermal operating limits will not be exceeded.

(f) Flux level and position data from the automatic traversing incore probe (ATIP) equipment are read into the computer. The computer evaluates the data and determines gain adjustment factors by which the LPRM amplifier gains can be altered to compensate for exposure-induced sensitivity loss. The LPRM amplifier gains are not to be physically altered except immediately prior to a whole core calibration using the ATIP system. The gain adjustment factor computations help to indicate to the operator when such a calibration procedure is necessary.

(g) Using the power distribution data, a distribution of fuel exposure increments from the time of previous power distribution calculation is determined and is used to update the distribution of cumulative fuel exposure. Each fuel bundle is identified by batch and location, and its exposure is stored for each of the axial segments used in the power distribution calculation. These data are printed out on operator demand. Exposure increments are determined periodically for each quarter-length section for each control rod. The corresponding cumulative exposure totals are periodically updated and printed out on operator demand.

(h) The exposure increment of each local power range monitor is determined periodically and is used to update both the cumulative ion chamber exposures and the correction factors for exposure-dependent LPRM sensitivity loss. These data are printed out on operator demand.

(i) The computer provides online capability to determine monthly and on-demand isotopic composition for each fuel bundle in the core. This evaluation consists of computing the weight of one neptunium, three uranium, and five plutonium isotopes, as well as the total uranium and total plutonium content. The isotopic composition is calculated and summed accordingly by bundles and batches.

(8) Reactor Operation Information (Monitor, Alarm, and Logging Programs)

(a) General

The processor is capable of checking each analog input variable against two types of limits for alarming purposes:

(i) Process alarm limits as determined by the computer during computation or as preprogrammed at some fixed value by the operator and

(ii) A reasonableness limit of the analog input signal level programmed.

The alarming sequence consists of an audible alarm, a console alarm, and a descriptive message for the variables that exceed process alarm limits. The processor provides the capability to alarm the main control room annunciator system in the event of abnormal PCS operation.

(b) Trip / Scram Data Recall Logging

The processor measures and stores the values of a set of analog variables at predefined intervals to provide a history of data. An on-demand request permits the operator to initiate printing of this data and to terminate the log printout when desired.

(c) Trend Logging

An analog trend capability is provided for logging the values of the operator-selected analog inputs and calculated variables. The periodicity of the log is limited to a nominal selection of intervals, which can be adjusted as desired by program control.

(d) Status Alarm

The status alarm of a point shall be updated with a time-after occurrence equal to the processing cycle of the point plus two seconds. A printed record of system alarms is provided which includes point description and time of occurrence.

(e) Alarm Logging

The alarm logs required by the associated process programs are printed. Alarm printouts inform the operator of computer system malfunctions, system operation exceeding acceptable limits, and unreasonable, off-normal, or failed input sensors.

(9) BOP Performance Calculation Programs

These programs perform calculations and logging of plant performance data not directly related to the nuclear system. The data stored by the BOP program is printed out on logs. The BOP periodic log gives hourly and daily

values for temperatures, power outputs, and flows associated with the main generator and turbines and with the Feedwater, Recirculation, and Reactor Water Cleanup Systems. The BOP monthly log contains monthly averages and accumulations for plant gross and net power outputs, load distributions, turbine heat rates, and fuel burnup. BOP performance calculations include flow calculations, electrical calculations, thermodynamic calculations, Nuclear Boiler System performance calculations, turbine cycle performance calculations, condenser calculation, feedwater heaters and moisture separators performance calculations, and unit performance calculations.

#### 7.7.1.5.1 Performance Monitoring and Control Subsystem

**General** — The PMCS provides nuclear steam supply (NSS) performance and prediction calculations, video display control, point log and alarm processing and balance of plant (BOP) performance calculations.

**NSS Performance Module** — The NSS performance module provides the reactor core performance information. The calculations performed are as follows:

- The local power density for every fuel assembly is calculated using plant inputs of pressure, temperature, flow, LPRM levels, control rod positions, and the calculated fuel exposure.

- Total core thermal power is calculated from a reactor heat balance. Iterative computational methods are used to establish a compatible relationship between the core coolant flow and core power distribution. The results are subsequently interpreted as power in specified axial segments for each fuel bundle in the core.

- After calculating the power distribution within the core, the computer uses appropriate reactor operating limit criteria to establish alarm trip settings for each LPRM channel. These settings are expressed as maximum acceptable LPRM values to which the actual scanned LPRM readings are compared. The scanned LPRM, when exceeding the alarm trip settings, will sound an alarm and thereby assist the operator to maintain core operation within permissible thermal limits established by the prescribed maximum fuel rod power density and minimum critical power ratio criteria. LPRM calibration constants are periodically calculated.

- The core power distribution calculation sequence is completed periodically and on demand. Subsequent to executing the program, the computer prints a periodic log for record purposes. Key operating parameters are evaluated based on power distribution and edited on the log.

- Each LPRM is scanned at an appropriate rate and, together with appropriate computational methods, provides nearly continuous reevaluation of core thermal limits with subsequent modification to the LPRM alarm trip settings based on the

new reactor operating level. The range of surveillance and the rapidity with which the computer responds to the reactor changes permit more rapid power maneuvering with the assurance that thermal operating limits will not be exceeded.

- Flux level and position data from the automatic fixed in-core probe (AFIP) equipment are read into the computer. The computer evaluates the data and determines gain adjustment factors by which the LPRM amplifier gains can be altered to compensate for exposure-induced sensitivity loss. The LPRM amplifier gains are not to be physically altered except immediately prior to a whole core calibration using the AFIP system. The gain adjustment factor computations help to indicate to the operator when such a calibration procedure is necessary.

- Using the power distribution data, a distribution of fuel exposure increments from the time of the previous power distribution calculation is determined and is used to update the distribution of cumulative fuel exposure. Each fuel bundle is identified by batch and location, and its exposure is stored for each of the axial segments used in the power distribution calculation. These data are printed out on operator demand. Exposure increments are determined periodically for each quarter-length section for each control rod. The corresponding cumulative exposure totals are periodically updated and printed on operator demand.

- The exposure increment of each local power range monitor is determined periodically and is used to update both the cumulative ion chamber exposures and the correction factor for exposure-dependent LPRM sensitivity loss. These data are printed out on operator demand.

**Video Display Control** — The video display control functions of the PMCS provides a major portion of the plant man-machine interface (MMI). This MMI consists of the input and output of all of the other PMCS modulated displayed on video display units (VDUs) in the main control room and at various other locations throughout the plant. Same of the VDUs are fitted with on-screen control devices for controlling non-safety-related systems and equipment.

### Point Log and Alarm Module

**General** — The Point Log and Alarm functions provide alarms and point data in the form of logs, summaries and group point displays, and a user interface to control point processing, logging, and alarming.

**Analog Variable Alarms**—The processor is capable of checking each analog input variable against two types of limits for alarming purposes:

- process alarm limits as determined by the computer during computation or as preprogrammed at some fixed value by the operator; and

- a reasonableness limit of the analog input signal level programmed.

The alarming sequence consists of an audible alarm, a console alarm, and a descriptive message for the variables that exceed process alarm limits. The processor provides the capability to alarm on the main control room annunciator system in the event of abnormal PCS operation.

**Status Alarm —** The status alarm of a point shall be updated with a time-after occurrence equal to the processing cycle of the point plus two seconds. A printed record of system alarms is provided which includes point description and time of occurrence.

**Alarm Logging —** The alarm logs required by the associated process programs are printed. Alarm printouts inform the operator of computer system malfunctions, system operation exceeding acceptable limits and unreasonable, off-normal or failed input sensors.

**Trip / Scram Data Recall Logging —**The processor measures and stores the values of a set of analog variables at predefined intervals to provide a history of data. An on-demand request permits the operator to initiate printing of this data and to terminate the log printout when desired.

**Trend Logging —** An analog trend capability is provided for logging the values of the operator-selected analog inputs and calculated variables. The periodicity of the log is limited to a nominal selection of intervals, which can be adjusted as desired by program control.

#### Balance of Plant Performance Calculation Programs

The balance of plant (BOP)programs perform calculations and logging of plant performance data not directly related to the nuclear system. The data stored by the BOP program is printed out on logs. The BOP periodic log gives hourly and daily values for temperatures, power outputs, and flows associated with the main generator and turbines, and with the Feedwater Control and Reactor Water Cleanup / Shutdown Cooling Systems. The BOP monthly log contains monthly averages and accumulations for plant gross and net power outputs, load distributions, turbine heat rates, and fuel burnup. The BOP performance calculations include flow calculations, electrical calculations, thermodynamic calculations, Nuclear Boiler System performance calculations, condenser calculation, feedwater heaters and moisture separators performance calculations and unit performance calculations.

### 7.7.1.5.2 Power Generation Control Subsystem

The Power Generation Control Subsystem (PGCS) is a top level controller that monitors the overall plant conditions, issues control commands to non-safety-related systems, and adjusts setpoints of lower level controllers to support automation of the normal plant startup, shutdown, and power range operations. The PGCS is a separate

function of the Process Computer System. The PGCS contains the algorithms for the automated control sequences associated with plant startup, shutdown and normal power range operation. The PGCS issues reactor command signals to the automatic power regulator (APR). The reactor power change algorithms are implemented in the APR.

In the automatic mode, the PGCS issues command signals to the turbine master controller which contains appropriate algorithms for automated sequences of turbine, feedwater, and related auxiliary systems. Command signals for setpoint adjustment of lower level controllers and for startup/shutdown of other systems required for plant operation are executed by the PGCS. The operator interfaces with the PGCS through a series of breakpoint controls to initiate automated sequences from the operator control console. For selected operations that are not automated, the PGCS prompts the operator to perform such operations. In the semi automatic mode, the PGCS provides guidance messages to the operator to carry out the startup, shutdown, and power range operations.

The PGCS is classified as a power generation system and is not required for safety. Safety-related events requiring control rod scram are sensed and controlled by the safety-related Reactor Protection System which is completely independent of the PGCS.

The PGCS interfaces with the operator's console to perform its designated functions. The operator's control console for PGCS consists of a series of breakpoint controls for a prescribed plant operation sequence. When all the prerequisites are satisfied for a prescribed breakpoint in a control sequence, a permissive is given and, upon verification by the operator, the operator initiates the prescribed sequence. The PGCS then initiates demand signals to the various system controllers to carry out the predefined control functions. (NOTE: For non-automated operations that are required during normal startup or shutdown (e.g., change of reactor mode switch status), automatic prompts are provided to the operator. Automated operations continue after the operator completes the prompted action manually.)

#### 7.7.1.5.3 Safety Evaluation

The Process Computer System is designed to provide the operator with certain categories of information and to supplement procedure requirements for control rod manipulation during reactor startup and shutdown. The system augments existing information from other systems such that the operator can start up, operate at power and shut down in an efficient manner. The PGCS function provides signals to the APR as explained in Subsection 7.7.1.5.2. However, this is a power generation function. Neither the Process Computer System nor its PGCS function initiate or control any engineered safeguard or safety-related system.

#### 7.7.1.5.4 Testing and Inspection Requirements

The Process Computer System has self-checking provisions. It performs diagnostic checks to determine the operability of certain portions of the system hardware and performs internal programming checks to verify that input signals and selected program computations are either within specific limits or within reasonable bounds.

#### 7.7.1.5.5 Instrumentation Requirements

There is no instrumentation in the Process Computer System other than the video display units (VDUs). Control of the Process Computer System is accomplished with on-screen methods and a few hard switches. System auxiliaries such as printers, plotters, and tape handlers have their own local controls.

### 7.7.1.6 Neutron Monitoring System—Non-Safety-Related Subsystems

#### 7.7.1.6.1 Automatic Traversing Incore Probe (ATIP)

This subsection describes the non-safety-related Automatic Traversing Incore Probe (ATIP) Subsystem of the Neutron Monitoring System (NMS). Safety-related NMS subsystems are discussed in Subsection 7.6.1.1.

(1) Description

The ATIP is comprised of three TIP machines, each with a neutron-sensitive sensor attached to the machine's flexible cable. Other than the sensor itself, each machine has a drive mechanism, a 20-position index mechanism, associated guide tube, and other parts. While not in use, the sensor is normally stored and shielded in a storage area inside the TIP room in the reactor building. During operation, the ATIP sensors are inserted, either manually or automatically, via guide tubing and through desired index positions to the designated LPRM assembly calibration tube. Each ATIP machine has designated number and locations of LPRM assemblies to cover, such that the ATIP sensor can travel to all LPRM locations assigned to this machine via the index mechanism of this machine. The LPRM assignments to the three machines are shown in Figure 7.7-10.

Flux readings along the axial length of the core are obtained by first inserting the sensor fully to the top of the calibration tube and then taking data as the sensor is withdrawn continuously from the top. Sensor flux reading, sensor axial positions data in the core, and LPRM location data are all sent to an ATIP control unit located in the control room, where the data can be stored. The data are then sent to the process computer for calibration and performance calculations. The whole ATIP scanning sequence and instructions are fully automated, with manual control available.

The index mechanism allows the use of a single sensor in any one of twenty different LPRM assemblies. There is a common LPRM location that allows all three ATIP scanning. This is for ATIP cross-machine calibration.

To protect against inadvertent radiation exposure from the ATIP System, the ATIP electronics and drive mechanism have built-in relay switches and mechanical motor stop switches to prevent the TIP detector from withdrawal into the drive mechanism. Alarm warnings are installed near the TIP room and the access way to the drywell to prevent personnel radiation exposure from the TIP (Subsection 12.3.2.3).

(2) Classification

The ATIP is non-safety-related as shown in Table 3.2-1. The subsystem is an operational system and has no safety function.

(3) Power Supply

The power for the ATIP is supplied from the instrument AC power source.

(4) Testability

The ATIP equipment is tested and calibrated using heat balance data and procedures described in the instruction manual.

(5) Environmental Considerations

The equipment and cabling located in the drywell are designed for continuous duty (Section 3.11).

(6) Operational Considerations

The ATIP can be operated during reactor operation to calibrate the LPRM channels. The subsystem has no safety setpoints.

### 7.7.1.6.2 Multi-Channel Rod Block Monitor (MRBM)

This subsection describes the non-safety-related Multi-Channel Rod Block Monitor (MRBM) Subsystem of the Neutron Monitoring System (NMS). Safety-related NMS subsystems are discussed in Subsection 7.6.1.1.

(1) System Identification

The MRBM Subsystem logic issues a rod block signal that is used in the RCIS logic to enforce rod blocks that prevent fuel damage by assuring that the minimum critical power ratio (MCPR) and maximum linear heat generation

rate (MLHGR) do not violate fuel thermal safety limits. Once a rod block is initiated, manual action is required by the operator to reset the system.

The MRBM microcomputer-based logic receives input signals from the local power range monitors (LPRMs) and the average power range monitors (APRMs) of the NMS. It also receives core flow data from the NMS, and control rod status data from the rod action and position information subsystem of the RCIS to determine when rod withdrawal blocks are required. The MRBM averages the LPRM signals to detect local power change during the rod withdrawal. If the averaged LPRM signal exceeds a preset rod block setpoint, a control rod block demand will be issued. The MRBM monitors many 4-by-4 fuel bundle regions in the core in which control rods are being withdrawn as a gang. Since it monitors more than one region, it is called the multi-channel rod block monitor. The rod block setpoint is a core-flow biased variable setpoint. The MRBM is a dual channel system not classified as a safety system.

(2) Classification

The MRBM is non-safety-related. Its activating interface is through the Rod Control and Information System (RCIS), which is also a non-safety-related system.

(3) Power Supply

The power supply for the MRBM is from the non-divisional 120 VAC UPS bus.

(4) Testability

The MRBM is a dual channel, independent subsystem of the NMS. One of the MRBM channels can be bypassed for testing or maintenance without affecting the overall MRBM function. Self-test features are employed to monitor failures in the microprocessor system. Test capabilities allow for calibration and trip output testing.

(5) Environmental and Operational Considerations

The MRBM is located in the control room adjacent to the APRM panels. It is physically and electrically isolated from the rest of the safety NMS subsystems. All interfaces with the safety NMS subsystems are via optical isolation.

### 7.7.1.7 Automatic Power Regulator System—Instrumentation and Controls

(1) Identification

The primary objective of the Automatic Power Regulator (APR) System is to control reactor power during reactor startup, power generation, and reactor shutdown, by appropriate commands to change rod positions, or to change reactor recirculation flow. The secondary objective of the APR System is to control the pressure regulator setpoint (or turbine bypass valve position) during reactor heatup and depressurization (e.g., to control the reactor cooldown rate). The APR System consists of redundant process controllers. Automatic power regulation is achieved by appropriate control algorithms for different phases of the reactor operation which include approach to criticality, heatup, reactor power increase, automatic load following, reactor power decrease, and reactor depressurization and cooldown. The APR System receives input from the plant process computer, the Power Generation Control System (Subsection 7.7.1.5.1), the Steam Bypass and Pressure Control System (Subsection 7.7.1.8), and the operator's control console. The output demand signals from the APR System are to the RCIS to position the control rods, to the RFC System to change reactor coolant recirculation flow, and to the SB&PC System for automatic load following operations. The PGS performs the overall plant startup, power operation, and shutdown functions. The APR System performs only those functions associated with reactor power changes and with pressure regulator setpoint (or turbine bypass valve position) changes during reactor heatup or depressurization. A simplified functional block diagram of the APR System is provided in Figure 7.7-11.

(2) Classification

The APR is classified as power generation system and is not required for safety. Safety events requiring control rod scram are sensed and controlled by the safety-related RPS, which is completely independent of the APR. The RPS is discussed in Section 7.2.

(3) Power Sources

The APR System digital controllers are powered by redundant uninterruptible non-Class 1E power supplies and sources. No single power failure shall result in the loss of any APR System function.

(4) Normal Operation

The APR System interfaces with the operator's console to perform its designed functions. The operator's control panel for automatic plant startup, power operation, and shutdown functions is part of the PGCS. This control panel consists of a series of breakpoint controls for a prescribed plant operation sequence. When all the prerequisites are satisfied for a prescribed breakpoint in a control sequence, a permissive is given and, upon verification by the

operator, the operator initiates the prescribed control sequence. The PGCS then initiates demand signals to various system controllers to carry out the predefined control functions. [Note: For non-automated operations that are required during normal startup or shutdown (e.g., change of Reactor Mode Switch status), automatic prompts are provided to the operator. Automated operations continue after the operator completes the prompted action manually.] The functions associated with reactor power control are performed by the APR System.

For reactor power control, the APR System contains algorithms that can change reactor power by control rod motions, or by reactor coolant recirculation flow changes, but not both at the same time. A prescribed control rod sequence is followed when manipulating control rods for reactor criticality, heatup, power changes, and automatic load following. Each of these functions has its own algorithm to achieve its designed objective. The control rod sequence can be updated from the process computer based on inputs from the reactor engineer. A predefined trajectory of power-flow is followed when controlling reactor power. The potentially unstable region of the power-flow map is avoided during plant startup, automatic load following, and shutdown. During automatic load following operation, the APR System interfaces with the SB&PC System to coordinate main turbine and reactor power changes for optimal performance.

(5) Abnormal Operation

The normal mode of operation of the APR System is automatic. If any system or component conditions are abnormal during execution of the prescribed sequences, the PGCS will be automatically switched into the manual mode and any operation in progress will be stopped. Alarms will be activated to alert the operator. With the APR System in manual mode, the operator can manipulate control rods and recirculation flow through the normal controls. A failure of the APR System will not prevent manual controls of reactor power, nor will it prevent safe shutdown of the reactor.

(6) Equipment

The APR System control functional logic is performed by redundant, microprocessor-based fault-tolerant digital controllers (FTDC). The FTDC performs many functions. It reads and validates inputs from the Non-Essential Multiplexing System (NEMS) interface once every sampling period. It performs the specific power control calculations and processes the pertinent alarm and interlock functions, then updates all system outputs to the NEMS. To prevent computational divergence among the redundant processing channels, each channel performs a comparison check of its calculated results

with the other redundant channels. The internal FTDC architecture features redundant multiplexing interfacing units for communications between the NEMS and the FTDC processing channels.

(7) Testability

The FTDC input and output communication interfaces are continuously functioning during normal power operation. Abnormal operation of these components can be detected during operation. In addition, the FTDC is equipped with self-test and online diagnostic capabilities for identifying and isolating failure of input/output devices, buses, power supplies, processors, and interprocessor communication paths. These online tests and diagnosis can be performed without disturbing the normal control functions of the APR System.

(8) Environmental Considerations

The APR System is not required for safety purposes, nor is it required to operate during or after any design basis accident. The system is required to operate in the normal plant environment for power generation purposes only. The APR System equipment is located in the main control room and subject to the normal control room environment as listed in Section 3.11.

(9) Operator Information and Operational Considerations

During operation of the APR System, the operator observes the performance of the plant via CRTs on the main console or on large screen displays in the main control room. The APR System can be switched into the manual mode by the operator, and a control sequence, which is in progress, can be stopped by the operator at any time. This will stop automatic reactor power changes. If any system or component conditions are abnormal during execution of the prescribed sequences, continued operation is stopped automatically and alarms will be activated to alert the operator. With the APR System in manual mode, the operator can manipulate control rods and recirculation flow through the normal controls. A failure of the APR System will not prevent manual controls of reactor power, nor will it prevent safe shutdown of the reactor.

(10) Setpoints

The APR System has no safety setpoints.

### 7.7.1.8 Steam Bypass & Pressure Control System—Instrumentation and Controls

(1) Identification

The primary objective of the Steam Bypass & Pressure Control (SB&PC) System is to control reactor vessel pressure during plant startup, power generation and shutdown modes of operation. This is accomplished through control of the turbine control and/or steam bypass valves, such that susceptibility to reactor trip, turbine-generator trip, main steam isolation and safety/relief valve opening is minimized.

Command signals for the turbine control valves and the steam bypass valves are generated by a triplicated FTDC using feedback signals from vessel pressure sensors. For normal operation, the turbine control valves regulate steam pressure. However, whenever the total steam flow demand from the pressure controller exceeds the effective turbine control valve steam flow demand, the SB&PC sends the excess steam flow directly to the main condenser, through the steam bypass valves.

Ability of the plant to follow grid-system load demands is enabled by adjusting reactor power level, by varying reactor recirculation flow (manually or automatically), or by moving control rods (manually or automatically). In response to the resulting steam production changes, the SB&PC adjusts the turbine control valves to accept the steam output change, thereby controlling steam pressure. In addition, when the reactor is automatically following grid-system load demands, the SB&PC permits an immediate steam flow response to fast changes in load demand, thus utilizing part of the stored energy in the vessel.

(2) Classification

The SB&PC System is a power generation system and is non-safety related.

(3) Power Sources

The SB&PC controls and bypass valves are powered by redundant uninterruptable non-Class 1E power supplies and sources. No single power failure will result in the loss of SB&PC System function. Upon failure of two or more channels in the controller, the turbine will trip.

(4) Normal Plant Operation

At steady-state plant operation, the SB&PC System maintains primary system pressure at a nearly constant value, to ensure optimum plant performance.

During normal operational plant maneuvers (pressure setpoint changes, level setpoint changes, recirculation flow changes), the SB&PC System provides responsive, stable performance to minimize vessel water level and neutron flux transients.

During plant startup and heatup, the SB&PC System provides for automatic control of the reactor vessel pressure. Independent control of reactor pressure and power is permitted, during reactor-vessel heatup, by varying steam bypass flow as the main turbine is brought up to speed and synchronized.

The SB&PC System also controls pressure during normal (MSIVs open) reactor shutdown to control the reactor cooling rate.

(5) Abnormal Plant Operation

Events which induce reactor trip present significant transients during which the SB&PC System must maintain steam pressure. These transients are characterized by large variations in vessel steam flow, core thermal-power output, and sometimes recirculation flow, all of which affect vessel water level. The SB&PC System is designed to respond quickly to stabilize system pressure and thus aid in the feedwater/level control in maintaining water level.

The SB&PC System is also designed for operation with other reactor control systems to avoid reactor trip after significant plant disturbances. Examples of such disturbances are loss of one feedwater pump, loss of three recirculation pumps, inadvertent opening of safety/relief valves or steam bypass valves, main turbine stop/control valve surveillance testing, and MSIV testing.

(6) Equipment

The SB&PC System control functional logic is performed by triplicated microprocessor-based FTDC similar to those used for the feedwater and recirculation flow control systems. It is therefore possible to lose one complete processing channel without impacting the system function. This also facilitates taking one channel out of service for maintenance or repair while the system is online. The IED and IBD are provided as Figures 7.7-12 and 7.7-13, respectively.

Controls and valves are designed such that steam flow is shut off upon loss of control system electrical power or hydraulic system pressure.

The pressure control function provides ABWR automatic load following by forcing the turbine control valves to remain under pressure control supervision, while enabling fast bypass opening for transient events requiring fast reduction in turbine steam flow.

The steam bypass function controls reactor pressure by modulating three automatically operated, regulating bypass valves in response to the bypass flow demand signal. This control mode is assumed under the following conditions:

(a) During reactor vessel heat-up to rated pressure.

(b) While the turbine is brought up to speed and synchronized.

(c) During power operation when reactor steam generation exceeds the turbine steam flow requirements.

(d) During plant load rejections and turbine-generator trips.

(e) During cooldown of the nuclear boiler.

(7) I&C Interface

The external signal interfaces for the SB&PC System are as follows:

(a) Narrow range dome pressure signals from the SB&PC System to the Recirculation Flow Control System.

(b) Equivalent load or steam flow feedback signal from the Turbine Control System (which is also a triplicated fault-tolerant digital controller).

(c) Signals to and from the main control room.

(d) Bypass hydraulic power supply trouble signal from the Turbine Bypass System to the SB&PC System.

(e) Output signals from the SB&PC System to the performance monitoring and control function of the process computer.

(f) Displayed variables and alarms from the SB&PC System to the main control room panel operator interface.

(g) Narrow and wide range pressure signals, MSIV position signals from the Nuclear Boiler System to the SB&PC System.

(h) Bypass valve position, servo current, position error and valve open and closed signals from the Turbine Bypass System.

(i) Emergency bypass valve fast opening signals and bypass valve flow demand signals from the SB&PC System to the Turbine Bypass System.

(j) Electric power from the non-Class 1E power supply to the SB&PC System.

(k) Pressure setpoint change requests/commands from the turbine master controller, for automatic startup and shutdown sequences.

(l) Governor-free demand signal to the reactor power compensator in the APR system.

(m) Reactor power compensation signal in accordance with speed error from the SB&PC System to the APR System.

(n) Main condenser vacuum low signal from the extraction system to the SB&PC System.

(8) Testability

The FTDC input and output communication interfaces are continuously functioning during normal power operation. Abnormal operation of these components can be detected during operation. In addition, the FTDC is equipped with self-test and online diagnostic capabilities for identifying and isolating failure of input/output devices, buses, power supplies, processors, and interprocessor communication paths. These online tests and diagnoses can be performed without disturbing the normal control functions of the SB&PC system.

(9) Environmental Considerations

The SB&PC System is not required for safety purposes, nor is it required to operate during or after any design basis accident. The system is required to operate in the normal plant environment for power generation purposes only. The SB&PC System equipment is located in the main control room and subject to the normal control room environment (Section 3.11).

(10) Operator Information

During operation of the SB&PC System, the operator may observe the performance of the plant via CRTs on the main control console or on large screen displays in the main control room. As described in (8) above, the self-test provision assures that all transducer/controller failures are indicated to the operator and maintenance personnel. The triplicated logic facilitates online repair of the controller circuit boards.

(11) Operational Considerations

During abnormal conditions that result in low main condenser vacuum, the steam bypass valves and MSIVs close to prevent positive pressure conditions that would rupture main condenser diaphragms. Manually operated provisions permit opening of the MSIVs (i.e., inhibit the closure function) during startup operation. This vacuum protection function bypass permits heatup of the main steamlines (up to the steam bypass valves and turbine stop

valves) before normal condenser vacuum is obtained and permits cold shutdown testing of the isolation valves.

The Steam Bypass System allows remote manual bypass operation in the normal sequence during plant startup and shutdown. This facilitates purge of the vessel and main steamlines of accumulated non-condensable gases early on in the startup process, and controls the rate of cooling during reactor shutdown to atmospheric pressures. Upon increasing pressure transients during such manual operation, the controls provide automatic override of the manual demand signal by the normal bypass demand. The system automatically returns to the manual demand signal when pressure transient causing the increased bypass demand is relieved.

In order to preserve steam for the main turbine gland seal functions, the bypass valves are inhibited from opening when either the inboard or outboard MSIVs close to their 90% positions. This bypass inhibit condition is annunciated in the main control room and must be manually reset by the operator. Any plant or component condition that inhibits bypass valve opening is annunciated.

(12) Setpoints

The SB&PC System has no safety setpoints because it is not a safety system. Preoperational setpoints and design parameters for the power generation functions are identified in the system design specifications (Subsection 1.1.3). Actual operational setpoints will be determined for each individual plant during startup testing.

### 7.7.1.9 Non-Essential Multiplexing System

The Non-Essential Multiplexing System(NEMS) is separate and distinct from the Essential Multiplexing System (EMS), though both are similar in design and architecture. Except for system interfaces and quality assurance requirements unique to Class 1E systems, specific design attributes discussed in Section 7A.2 pertain to the NEMS as well. Both systems are fully described in their subsection design specifications available from the Master Parts List referenced in Subsection 1.1.3. This subsection describes those features which are unique to the NEMS.

(1) System Description

The NEMS provides distributed control and instrumentation data communication networks to support the monitoring and control of interfacing plant power generation (non-safety-related) systems. [The EMS performs the same function for the protection (safety-related) systems.] The NEMS provides all the electrical devices and circuitry (such as multiplexing

units, data transmission line and transmission controllers), between sensors, display devices, controllers and actuators, which are defined by other plant systems. The NEMS also includes the associated data acquisition and communication software required to support its function of transmitting plant-wide data for distributed control and monitoring.

The NEMS acquires both analog and digital signals from remote process sensors and discrete monitors located within a plant, and multiplexes the signals to a central control room to drive annunciators, monitors and recorders, and to send signals, and output control signals are multiplexed to actuators, valves, motor drives and other control equipment in the plant associated with non-safety-related systems.

Consistent with fault-tolerant (triplicated) digital control systems utilized in feedwater control, reactor recirculation flow control and steam bypass and pressure regulation, the NEMS is also triplicated for these systems interfaces, as appropriate, each with its own independent control.

The remaining communication functions of the NEMS provides the following system functions:

(a) Acquires non-safety-related data (e.g., sensed input and equipment status signals) throughout the plant.

(b) Conditions, formats and transmits signals via fiber optics to displays, controllers, and the PCS.

(c) Receives signals via fiber optics, then multiplexes and prepares them for use in interfacing non-safety-related equipment as required.

(d) Formats and transmits processed control signals via fiber optics to actuator circuits, and then converts the fiber optic control signals to electrical signals for the actuator circuits.

(2) System Interface

The NEMS interfaces with the following systems, which are all non-safety-related:

— Reactor

— Nuclear Boiler (non-safety-related portion)

— Reactor Recirculation

— Rod Control

— Feedwater Control (including feedwater pump turbine)

— Recirculation Flow Control

— Steam Bypass and Pressure Control

— Process Computer

— Power Generation Control

— Process Radiation Monitoring (non-safety-related portion)

— Area Radiation Monitoring

— Dust Radiation Monitoring

— Refueling and Reactor Servicing

— Reactor Water Cleanup

— Fuel Pool Cooling and Cleanup

— Suppression Pool Cleanup

— Control Complex

— Makeup Water (purified, condensated)

— HVAC Normal Cooling Water

— Ultimate Heat Sink

— Turbine Service Water

— Steam and Heated Water

— Compressed Gas

— Sampling

— Condensate Demineralizer / Filter Facility

— Radwaste (includes Offgas)

— Turbine Bypass

— Turbine Control

— Feedwater Condensate Water

— Heater Drain

— Lubricating Oil

— Turbine Gland Steam

— Extraction

— Main Generator

— HVAC-Reactor Building

— HVAC-Other Buildings

— Electrical Power Distribution (non-safety-related portion)

— Annunciator

(3) Classification

The NEMs, of itself, is neither a power generation system nor a protection system. It is a support system utilized for assimilation, transmission and interpretation of data for power generation (non-safety-related) systems and their associated sensors, actuators and interconnections. It is classified as non-safety-related.

(4) Power Sources

The NEMS receives its power from three separate non-Class 1E distribution panels from the non-Class 1E 120 VAC UPS. This redundancy allows the NEMS to supply triplicated logic functions such that any single failure in the system power supplies will not cause the loss of the validated outputs to the interfacing actuators and to the monitors and displays.

(5) Equipment

The hardware and “firmware” architectures for the NEMS are the same as those of the EMS, which are described in Appendix 7A [see the response to NRC Requests (10) and (11) of Section 7A.2].

(6) Testability

The EMS test features described in Appendix 7A, Section 7A.2, Items (3), (4) and (6) are generally equivalent for the NEMS, except that the NEMS does not interface with, nor rely upon, the SSLC [see the response to NRC Request (6)

of Section 7A.2]. Also, the NEMS self-test features include the analog fault-tolerant voting system unique to the control systems employing logic.

(7) Environmental Considerations

The NEMS is not required for safety purposes, nor is it required to operate after the design basis accident. Its support function serves power generation purposes only and it is designed to operate in the normal plant environment.

(8) Operational Considerations

The system automatically initiates for both cold and warm starts. No operator actions are required in that the system is capable of self-starting following power interruptions, or any other single failure, including any single processor failure. After repairs or replacements are performed, the system automatically re-initializes to normal status when power is restored to any unit and automatically resets any alarms.

(9) Operator Information

The self-test provisions are designed to alert the operator to system anomalies via interfaces with the process computer and the annunciator. Problems significant enough to cause system channel failures are annunciated separately from those which allow continued operation. The circuitry is designed such that no control output or alarm is inadvertently activated during system initialization or shutdown. For such events, control outputs change to predetermined fail-safe outputs.

### 7.7.1.10 Fuel Pool Cooling and Cleanup System—Instrumentation and Controls

(1) System Identification

The Fuel Pool Cooling and Cleanup System is non-safety-related. Instrumentation and control is supplied to monitor and control the fuel pool temperature. The filter / demineralizer portion is non-safety-related. The instrumentation is for plant equipment protection.

The Fuel Pool Cooling and Cleanup System operates continuously on all plant modes. Evaporative losses in the system are replaced by the condensate system. If the heat load should become excessive, the Residual Heat Removal System is operated in parallel with this system to remove the excess heat load when the reactor is in shutdown condition. The arrangement of equipment and control devices is shown in the P&ID (Figure 9.1-1). The interlock block diagram is shown in Figure 7.7-14.

(2) Power Sources

Although the system is non-safety-related, it is considered to be a plant investment protection (PIP) load. Each of the two channels receives its power from separate PIP buses, backed by the combustion turbine generator. DC control power also comes from separate battery backed buses.

(3) Equipment Design

The cooling loop components of the Fuel Pool Cooling System have been designed to Seismic Category I requirements.

(a) Circuit Description

Temperature indication (alarm high) and level indication (alarm both high and low) are provided for the pools. The surge tank is also provided with level indication, alarm high and low.

Surge tank low-low level trip will automatically shut off the fuel pool pumps as described in Section 9.1.

The filter/demineralizer controls are carried out by a process control subsystem. Discussion of circuit design is not presented, since the total failure or malfunction of the subject control subsystem does not involve any safety function or ramification. The logic provided within the controller activates and carries out process activities such as backwashing, precoating, and filtering, based on the process variable condition.

(b) Bypass and Interlocks

Bypass valves and interlocks for the fuel pool cooling pumps are provided in this system. Each of the two pumps are interlocked to stop under the following conditions: (1) skimmer surge tank low-low level; or (2) the other pump is running and there is a low pump suction pressure or low pump discharge flow.

(c) Redundancy and Diversity

The cooling portion of the spent Fuel Pool Cooling and Cleanup System is redundant (i.e., these are two independent cooling loops, each capable of providing the required cooling for a normal quantity of fuel). Each of the two FPC heat exchangers is serviced by independent RCW loops. The RHR System can be used as a backup to cool the pool.

(d) Testability

The system is designed to remove decay heat load in the fuel pool during normal plan operation or at all other times. It is therefore fully testable at any time.

(e) Environment Considerations

Environmental conditions are the same for the normal condition and the accident condition because there are no high-energy systems in the area (Section 3.11).

(f) Operational Considerations

There are no special operating considerations.

### 7.7.1.11 Other Non-Safety-Related Control Systems

The following non-safety-related control systems are described in other Tier 2 subsections as indicated.

| System | Subsection |
|---|---|
| Fire Protection | 9.5.1 |
| Offgas/Radwaste | 11.2, 11.3, 11.4 |
| Drywell Cooling | 9.4.8 |
| Sampling | 9.3.2 |
| Instrument Air | 9.3.6 |
| Makeup Water | 9.2.3 |
| Atmospheric Control | 6.2.5 |

## 7.7.2 Analysis

The purpose of this subsection is to:

(1) Demonstrate by direct or referenced analysis that the subject-described systems are not required for any plant safety function.

(2) Demonstrate by direct or referenced analysis that the plant protection systems described elsewhere are capable of coping with all failure modes of the subject control system.

In response to item (1) above, the following is cited: upon considering the design basis, descriptions, and evaluations presented here and elsewhere throughout the document relative to the subject system, it can be concluded that these systems do not perform any safety-related function.

Design Basis: Refer to Subsection 7.1.1.

Description: Refer to Subsection 7.7.1.

The individual system analysis in this section concludes that the subject systems are not required for any plant safety action.

For consideration of item (2), above, it is necessary to refer to the safety evaluations in Chapter 15. In that chapter it is first shown that the subject systems are not utilized to provide any DBA safety function. Safety functions, where required, are provided by other qualified systems. For expected or abnormal transient incidents following the single operator error (SOE) or single component failure (SCF) criteria, protective functions are also shown to be provided by other systems. The expected or abnormal transients cited are the limiting events for the subject systems.

### 7.7.2.1 Nuclear Boiler System—Reactor Vessel Instrumentation

#### 7.7.2.1.1 General Functional Requirements Conformance

The reactor vessel instrumentation of the Nuclear Boiler System (NBS) is designed to provide redundant or augmented information to the existing information required from the engineered safeguards and safety-related systems. None of this non-safety-related instrumentation is required to initiate or control any engineered safeguard or safety-related system function.

#### 7.7.2.1.2 Specific Regulatory Requirements Conformance

Table 7.1-2 identifies the non-safety-related control systems and the associated codes and standards applied in accordance with Section 7.7 of the Standard Review Plan for BWRs. 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) General Design Criteria (GDC)

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

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

(2) Regulatory Guides (RGs)

In accordance with the Standard Review Plan for Section 7.7 and with Table 7.1-2, only RG 1.151(Instrument Sensing Lines) need be addressed for the ABWR.

(a) **Criteria***:* RG 1.151— "Instrument Sensing Lines"

(b) **Conformance:** There are four independent sets of instrument lines which are mechanically separated into each of the four instrument divisions of the NBS (see Figure 5.1-3, NBS P&ID). Each of the four instrument lines interfaces with sensors assigned to each of the four Class 1E electrical divisions for safety-related systems.

There are also non-Class 1E instruments that derive their input for the reactor vessel instrumentation portion of the NBS from these lines. There is no safety-related controlling function involved in this instrumentation and it is entirely separate (including its own MUX system) from the safety-related instruments and their associated systems.

The safety-related instrumentation provides vessel pressure and water level sensing for all protection systems. These instruments are arranged in two-out-of-four logic combinations and their signals are shared by both safety-related and non-safety-related systems. All of these signals are multiplexed and passed through fiber-optic media before entering the voting logic of the redundant divisions of the safety-related systems; or of non-safety-related systems which make up the various networks. Separation and isolation is thus preserved both mechanically and electrically in accordance with IEEE 279 and Regulatory Guide 1.75.

With four independent sensing lines and four independent electrical and mechanical divisions, the two-out-of-four voting logic assures no individual sensing line failure could prevent proper action of a protection system. When a system input channel is bypassed, the logic reverts to two-out-of-three.

The NBS instrument lines are not exposed to cold temperatures and are designed to meet the ASME Code requirements of Regulatory Guide 1.151 and ISA S67.02.

The Nuclear Boiler System is thus in full compliance with these criteria.

### 7.7.2.2 Rod Control and Information System—Instrumentation and Controls

#### 7.7.2.2.1 General Functional Requirements Conformance

The circuitry described for the Rod Control and Information System (RCIS) is completely independent of the circuitry controlling the scram valves. This separation of

the scram and normal rod control functions prevents failures in the rod control and information circuitry from affecting the scram circuitry. The scram circuitry is discussed in Section 7.2. The effectiveness of a reactor scram is not impaired by the malfunctioning of any one control rod drive circuitry. It can be concluded that no single failure in the RCIS can result in the prevention of a reactor scram, and that repair, adjustment, or maintenance of the RCIS components does not affect the scram circuitry.

Chapter 15 examines the various failure mode considerations for this system. The expected and abnormal transients and accident events analyzed envelope the failure modes associated with this system's components.

#### 7.7.2.2.2 Specific Regulatory Requirements Conformance

Table 7.1-2 identifies the non-safety-related control systems and the associated codes and standards applied in accordance with Section 7.7 of the Standard Review Plan for BWRs. 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) General Design Criteria (GDC)

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

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

(2) Regulatory Guides (RGs)

In accordance with the Standard Review Plan for Section 7.7 and with Table 7.1-2, only RG 1.151 ("Instrument Sensing Lines") need be addressed for the ABWR. However, the RCIS has no direct interface with the instrument lines, so this guide is not applicable. The criteria of this guide are discussed in relation to the NBS in Subsection 7.7.2.1.2 (2).

### 7.7.2.3 Recirculation Flow Control System—Instrumentation and Controls

#### 7.7.2.3.1 General Functional Requirements Conformance

The Recirculation Flow Control (RFC) System consists of the triplicated RFC process controller, adjustable speed drives, switches, sensors, and alarm devices provided for operational manipulation of the ten reactor internal pumps (RIPs) and the surveillance of associated equipment.

Although not required to meet single-failure criteria, each processing channel of the triply redundant digital processor receives its respective power input from an uninterruptible, independent source of the instrument and control power supply system. The allocation of the RIP equipment on four power buses is such that, on loss of any single power bus, a maximum of three can be affected.

System single failure or single operator errors are evaluated in the transient analysis of Chapter 15. It is shown that no malfunction in the RFC System can cause a transient sufficient to cause significant damage to the fuel barrier or exceed the nuclear system pressure limits.

#### 7.7.2.3.2 Specific Regulatory Requirements Conformance

Table 7.1-2 identifies the non-safety-related control systems and the associated codes and standards applied in accordance with Section 7.7 of the Standard Review Plan for BWRs. 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) General Design Criteria (GDC)

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

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

(2) Regulatory Guides (RGs)

In accordance with the Standard Review Plan for Section 7.7 and with Table 7.1-2, only RG 1.151(“Instrument Sensing Lines”) need be addressed for the RFC. The RFC System receives signals from sensors on vessel instrument lines via the Nuclear Boiler System. The criteria of this guide are discussed in relation to the NBS in Subsection 7.7.2.1.2 (2).

### 7.7.2.4 Feedwater Control System—Instrumentation and Controls

#### 7.7.2.4.1 General Functional Requirements Conformance

The Feedwater Control (FDWC) System is not a safety-related system and is not required for safe shutdown of the plant. It is a power generation system for purposes of maintaining proper vessel water level. Its operation range is from water level 8 (L8) to water level 2 (L2). Should the vessel level rise too high (L8), the feedwater pumps and plant main turbine would be tripped. This is an equipment protective action which would result in reactor shutdown by the RPS as outlined in Section 7.2. Lowering of the vessel level would also result in action of the RPS and ECCS to shut down the reactor.

The system digital controllers and process measurement equipment are powered by non-Class 1E redundant uninterruptible power supplies. No single power supply failure shall result in the loss of any FDWC System function.

Chapter 15 examines the various failure modes for this system relative to plant safety and operational effects.

#### 7.7.2.4.2 Specific Regulatory Requirements Conformance

Table 7.1-2 identifies the non-safety-related control systems and the associated codes and standards applied in accordance with Section 7.7 of the Standard Review Plan for BWRs. 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) General Design Criteria (GDC)

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

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

(2) Regulatory Guides (RGs)

In accordance with the Standard Review Plan for Section 7.7 and with Table 7.1-2, only RG 1.151 (“Instrument Sensing Lines”) need be addressed for the ABWR. The FDWC receives signals from sensors on vessel instrument lines via the NBS. The criteria of this guide are discussed in relation to the NBS in Subsection 7.7.2.1.2 (2).

### 7.7.2.5 Process Computer System—Instrumentation and Controls

#### 7.7.2.5.1 General Functional Requirements Conformance

The Process Computer System (PCS) is designed to provide the operator with certain categories of information and to supplement procedure requirements for control rod manipulation during reactor startup and shutdown. The system augments existing information from other systems such that the operator can start up, operate at power, and shut down in an efficient manner. The PGCC function provides signals to the Automated Power Regulator (APR) as explained in Subsection 7.7.1.5.1. However, this is a power generation function. Neither the PCS nor its PGCC function initiate or control any engineered safeguard or safety-related system.

#### 7.7.2.5.2 Specific Regulatory Requirements Conformance

Table 7.1-2 identifies the non-safety-related control systems and the associated codes and standards applied in accordance with Section 7.7 of the Standard Review Plan for BWRs. However, since the computer has no controlling function, none of the listed criteria is applicable.

Input data for the PCS are derived from both Class 1E and non-Class 1E sources. All such interfaces are optically isolated, where necessary, to assure the proper separation of redundant signals in accordance with Regulatory Guide 1.75.

### 7.7.2.6 Neutron Monitoring System—ATIP Subsystem Instrumentation and Controls

#### 7.7.2.6.1 General Functional Requirements Conformance

The ATIP Subsystem of the Neutron Monitoring System is non-safety-related and is situated separately from safety-related hardware. It is used as a means of calibrating LPRM instrument channels and has no controlling function with other systems.

#### 7.7.2.6.2 Specific Regulatory Requirements Conformance

Table 7.1-2 identifies the non-safety-related control systems and the associated codes and standards applied in accordance with Section 7.7 of the Standard Review Plan for BWRs. However, since the ATIP System has no controlling function, and is used only for calibration of the LPRMs, none of the listed criteria is applicable.

### 7.7.2.7 Automatic Power Regulator System—Instrumentation and Controls

#### 7.7.2.7.1 General Functional Requirements Conformance

The Automatic Power Regulator (APR) System is a power generation system in that it receives command signals from the Power Generation System and the SB&PC System; then controls reactor power by manipulating control rods (via the RCIS) or recirculation flow (via the RFC System). The protective scram function is entirely separate (via the RPS).

The APR is classified as non-safety-related and does not interface with any engineered safeguard or safety-related system.

#### 7.7.2.7.2 Specific Regulatory Requirements Conformance

Table 7.1-2 identifies the non-safety-related control systems and the associated codes and standards applied in accordance with Section 7.7 of the Standard Review Plan for BWRs. 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) General Design Criteria (GDC)

(a) **Criteria:** GDCs 13 and 19

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

(2) Regulatory Guides (RGs)

In accordance with the Standard Review Plan for Section 7.7 and with Table 7.1-2, only RG 1.151 (“Instrument Sensing Lines”) need be addressed for the ABWR. The APR System does not have any direct interface with the instrument lines; therefore, this guide is not applicable.

### 7.7.2.8 Steam Bypass and Pressure Control System—Instrumentation and Controls

#### 7.7.2.8.1 General Functional Requirements Conformance

The Steam Bypass & Pressure Control (SB&PC) System is a power generation system in that it inputs information to the Automatic Power Regulator, which, in turn, controls reactor power by manipulating control rods (via the RCIS) or recirculation flow (via the RFC System). The protective scram function is entirely separate (via the RPS).

The SB&PC is classified as non-safety-related and does not interface with any engineered safeguard or safety-related system.

#### 7.7.2.8.2 Specific Regulatory Requirements Conformance

Table 7.1-2 identifies the non-safety-related control systems and the associated codes and standards applied in accordance with Section 7.7 of the Standard Review Plan for BWRs. 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) General Design Criteria (GDC)

(a) **Criteria:** GDCs 13 and 19

(b) **Conformance:** The SB&PC System is in compliance with these GDCs, in part, or as a whole, as applicable. The GDCs are generally addressed in Subsection 3.1.2

(2) Regulatory Guides (RGs)

In accordance with the Standard Review Plan for Section 7.7 and with Table 7.1-2, only RG 1.151 (“Instrument Sensing Lines”) need be addressed for the ABWR.

(a) **Criteria:** Regulatory Guide 1.151—Instrument Sensing Lines

(b) **Conformance:** The SB&PC interfaces with sensors connected to instrument lines on both the reactor and the turbine. The reactor instrument line interface is via the Nuclear Boiler System, which is in full compliance with this guide as discussed in Subsection 7.7.2.1.2 (2).

There are four independent turbine instrument lines, which contain turbine first-stage pressure sensors as part of the Turbine Control System, in addition to the non-Class 1E sensors associated with the SB&PC System. The first-stage turbine pressure signals are used as bypass interlocks for the turbine control valve fast closure and turbine stop valve closure scram functions [Subsection 7.2.1.1.4.2 (6) (d)]. No single failure can cause this function to be disabled. In addition, since the Turbine Building itself is a non-seismic structure, these scram functions are backed up by diverse reactor variables [reactor high pressure and high flux (via NMS)] which will independently initiate scram, should the turbine signals be lost. Therefore, no event associated with turbine instrument lines can cause an action requiring scram, while at the same time disabling the scram function. The SB&PC System fully complies with Regulatory Guide 1.151.

### 7.7.2.9 Non-Essential Multiplexing System—Instrumentation and Controls

#### 7.7.2.9.1 General Requirements Conformance

The NEMS, of itself, is neither a power generation system nor a protection system. It is a support system utilized for assimilation, transmission and interpretation of data for power generation (non-safety-related) systems and their associated sensors, actuators and interconnections. It is classified as non-safety-related and does not interface with any engineered safeguard or safety-related system except for isolated alarms for annunciation.

The NEMS is an integral part of the power generation systems which it supports. As such, it meets the same functional requirements imposed on those systems. Although not required to meet the single-failure criterion, the system is redundant and receives its power from redundant, highly reliable power sources such that no single failure will cause its basic function to fail.

### 7.7.2.9.2 Specific Regulatory Requirements Conformance

Table 7.1-2 identifies the non-safety-related control systems and the associated codes and standards applied in accordance with Section 7.7 of the Standard Review Plan. However, as mentioned above, the NEMS is not a separate control system subject to separate review, but is the data communication vehicle for virtually all of the non-safety-related systems. It provides specific enhancement for all control systems in their conformance with GDCs 13 and 19.

## 7.7.2.10 Fuel Pool Cooling and Cleanup System Instrumentation and Control

### 7.7.2.10.1 General Requirements Conformance

The FPC System is neither a power generation system nor a protection system. It is an independent system designed to monitor and control the fuel pool temperature and to maintain the water quality of the pool.

The system has two active redundant loops which receive their power from independent combustion turbine generator (CTG) backed buses. Therefore, no single failure will cause its basic function to fail. Also, the RHR System is given credit to provide supplemental pool cooling.

### 7.7.2.10.2 Specific Regulatory Requirements Conformance

Table 7.1-2 indentifies the non-safety-related control systems and the associated codes and standards applied in accordance with Section 7.7 of 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) General Design Criteria (GDC)

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

(b) **Conformance:** The FPC System is in compliance with these GDCs, in part, or as a whole, as applicable. The GDCs are generally addressed in subsection 3.1.2. Instrumentation and controls are provided in the control room. The filter / demineralizer portion is controllable from the local panels. Since the system is not associated with reactor shutdown, there are no controls needed nor provided in the remote shutdown facility.

(2) Regulatory Guide (RGs)

In accordance with the Standard Review Plan for Section 7.7 and with Table 7.1-2, only Regulatory Guide 1.151 (“Instrument Sensing Lines”) need be addressed for the ABWR. The FPC instrument lines are not exposed to cold

temperatures and are designed to meet the ASME code requirements of RG 1.151 and ISA S67.02. The FPC System is thus in full compliance with these criteria.

### 7.7.2.11 Other Non-Safety-Related Control Systems

The following non-safety-related control systems are described in other subsections of the SSAR as indicated.

| System | Subsection |
|---|---|
| Fire Protection | 9.5.1 |
| Offgas/Radwaste | 11.2, 11.3, 11.4 |
| Drywell Cooling | 9.4.8 |
| Sampling | 9.3.2 |
| Instrument Air | 9.3.6 |
| Makeup Water | 9.2.3 |
| Atmospheric Control | 6.2.5 |
| Reactor Water Cleanup | 5.4.8 |

## Table 7.7-1 RCIS Module Operation Environment

| | Minimum | Design Center | Maximum | (Units) |
|---|---|---|---|---|
| (1) Temperature | | | | |
| (a) Operating | –10 | 20 | 50 | °C |
| (b) Non-operating | –20 | | 60 | °C |
| (2) Relative Humidity (Non-condensing) | | | | |
| (a) Operating | 10 | 50 | 90 | %RH |
| (b) Non-operating | 5 | | 95 | %RH |
| (3) Atmospheric Pressure | | | | |
| (a) Static | 0.09 | 0.1 | 0.11 | MPa |
| (4) Radiation: | Operating gamma dose rate [0.036 mGy (carbon)/h] integrated dose over qualified life [100 Gy (carbon)] | | | |
| (5) Seismic: | All RCIS modules and cabinets are designed to operate correctly during accelerations of 2 g's in any plane for one minute over the frequency range of 0.1 to 30 Hz. All RCIS cabinets are designed to be capable of withstanding an acceleration of 5 g's in any plane for one minute over the frequency range of 0.1 to 30 Hz without sustaining damage. | | | |

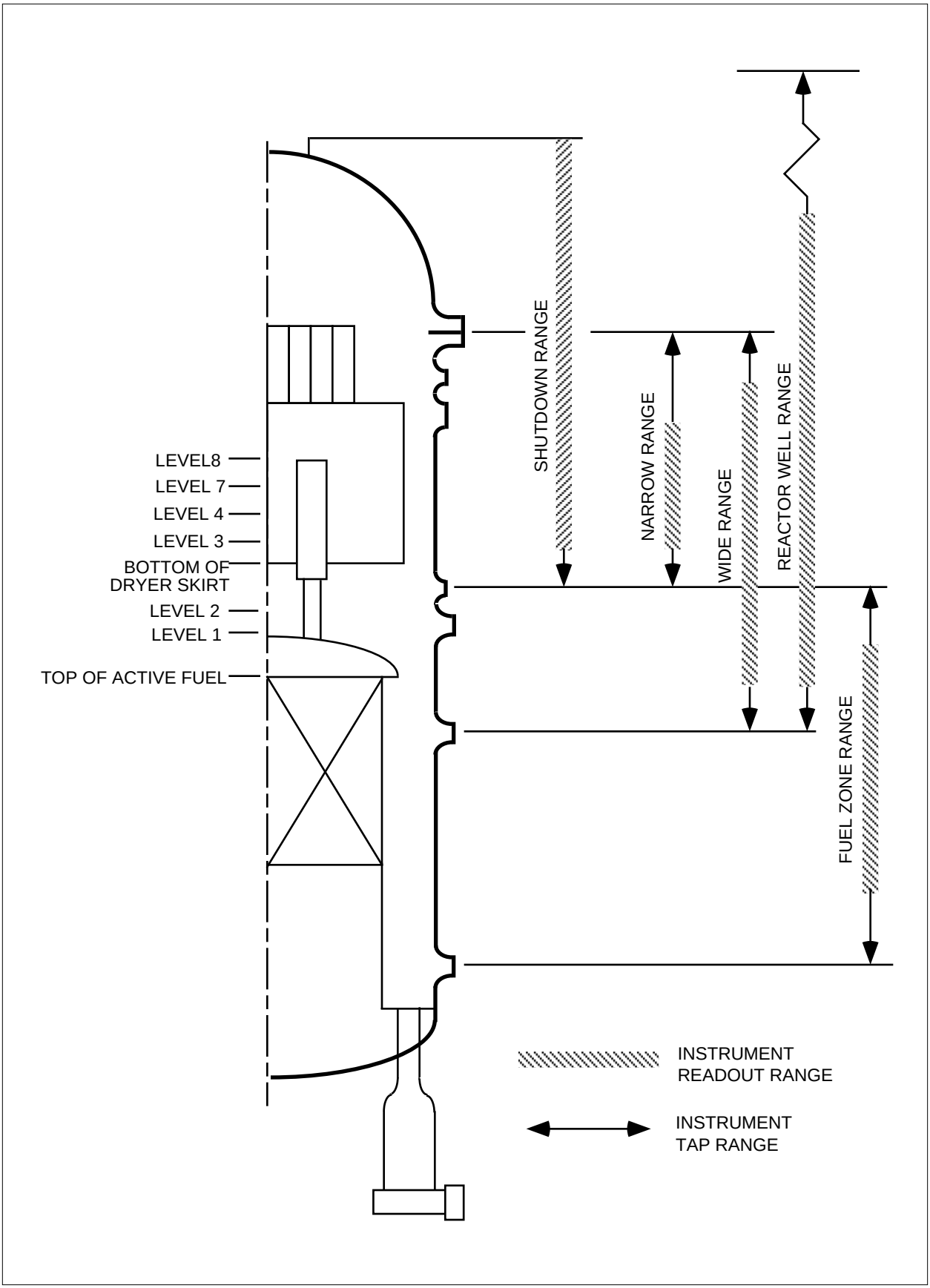



**Figure 7.7-1 Water Level Range Definition**

**The following figures are located in Chapter 21:**

**Figure 7.7-2 Rod Control and Information System IED (Sheets 1-5)**

**Figure 7.7-3 Rod Control and Information System IBD (Sheets 1-87)**

**Figure 7.7-4 Control Rod Drive System IBD (Sheets 1-8)**

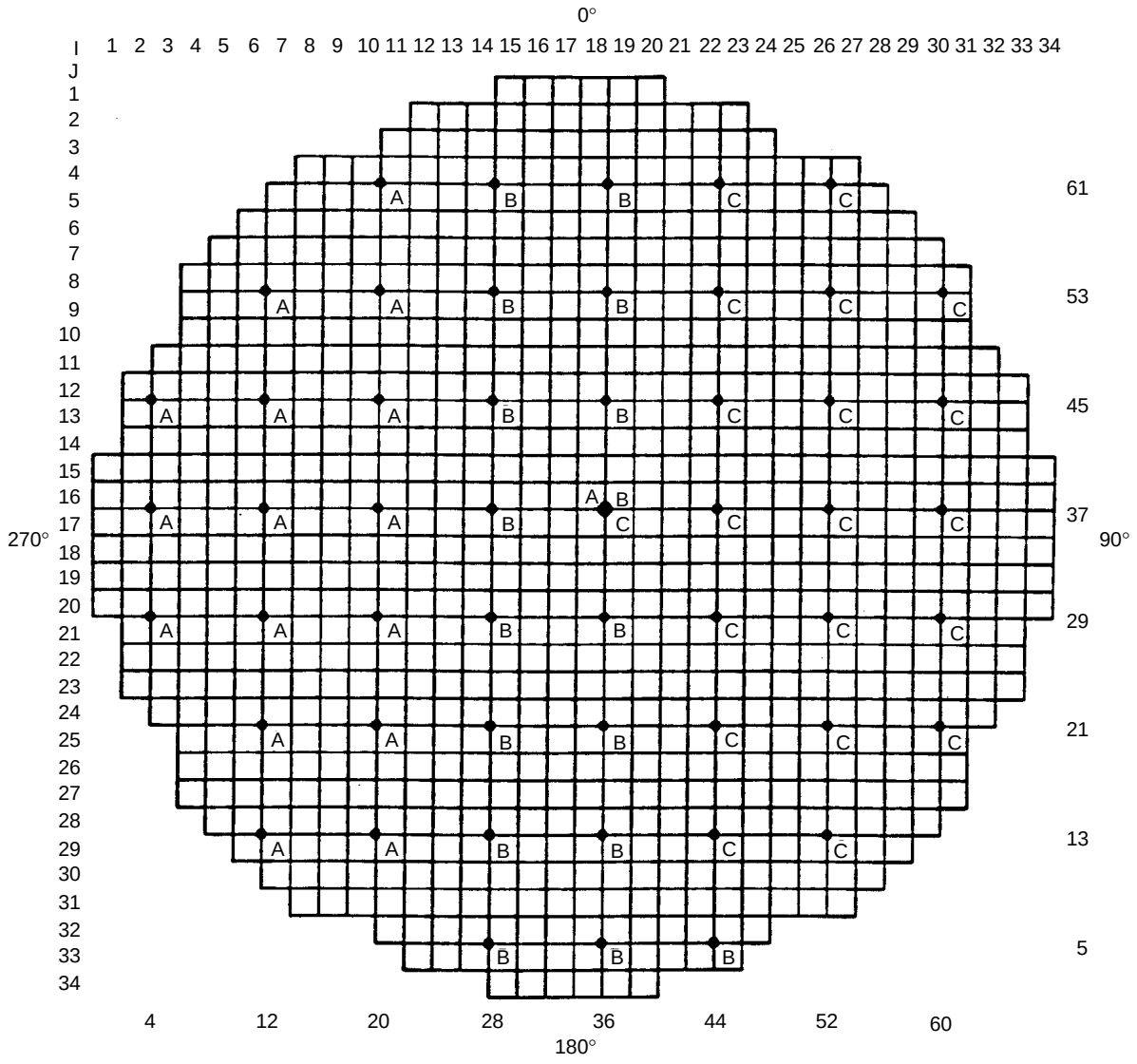
**Figure 7.7-5 Recirculation Flow Control System IED (Sheets 1-2)**

**Figure 7.7-6 Not Used**

**Figure 7.7-7 Recirculation Flow Control System IBD (Sheets 1-9)**

**Figure 7.7-8 Feedwater Control System IED (Sheets 1-3)**

**Figure 7.7-9 Feedwater Control System IBD (Sheets 1-14)**




(LETTERS SHOWN IN THE CORE MAP REFER TO ATIP MACHINES A, B, C)
(I, J COORDINATES REFER TO 3-D MONITOR CODE CORE COORDINATES)

**Figure 7.7-10 Assignment of LPRM Strings to TIP Machines**

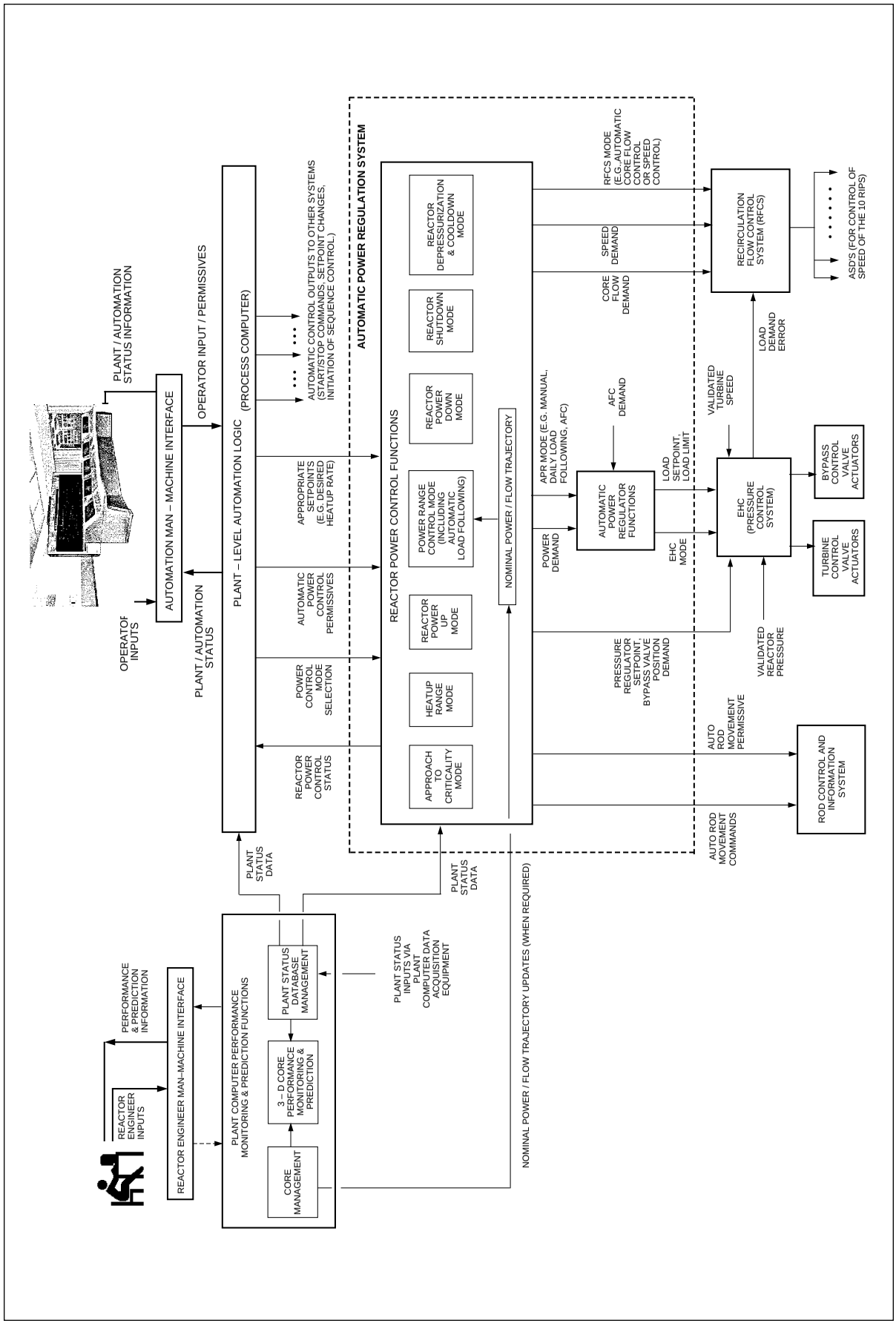



**Figure 7.7-11 Simplified Functional Diagram of the Automatic Power Regulation System**

**The following figures are located in Chapter 21:**

**Figure 7.7-12 Steam Bypass and Pressure Control System IED (Sheets 1-2)**

**Figure 7.7-13 Steam Bypass and Pressure Control System IBD (Sheets 1-5)**

**Figure 7.7-14 Fuel Pool Cooling and Cleanup System IBD (Sheets 1–8)**

# 7.8 COL License Information

## 7.8.1 Effects of Station Blackout on the HVAC

A temperature heat rise analysis shall be provided by the COL applicant for the station blackout (SBO) scenario applied to the control room on consideration of the environmental temperatures unique to the plant location (see Chapter 20, NRC Question 420.14).

## 7.8.2 Electrostatic Discharge on Exposed Equipment Components

The response to NRC Question 420.90 provides recommendations for limiting the effects of electrostatic discharge (ESD) at keyboards, keyed switches and other exposed equipment. The COL applicant shall provide assurance that the grounding and shielding techniques are consistent with these recommendations, or provide an acceptable alternative plan for controlling ESD (see Chapter 20, NRC Question 420.90).

## 7.8.3 Localized High Heat Spots in Semiconductor Materials for Computing Devices

The response to NRC Question 420.92 provides recommendations for limiting high current densities which could result in localized heat spots in semiconductor materials used in computing devices. The COL applicant shall provide assurance that these recommendations are followed, or an acceptable alternative is presented, by the selected equipment vendor(s). To ensure that adequate compensation for heat rise is incorporated into the design, a thermal analysis shall be performed at the circuit board, instrument and panel design stages (see Chapter 20, NRC Question 420.92).

# 7A Design Response to Appendix B, ABWR LRB Instrumentation and Controls

## 7A.1 Introduction

The instrumentation and control (I&C) systems of the ABWR use state-of-the-art fiber optics, multiplexing and computer controls.

In Appendix B to the GE Advanced Boiling Water Reactor Licensing Review Bases (LRB), dated August, 1987, the NRC staff indicated that guidance in this area had not been developed. However, GE committed to address the standards and criteria currently specified in the SRP, and to use the documents and criteria identified in Appendix B.

The NRC requested considerable additional information specific to this equipment in Appendix B. The NRC requests, along with GE's responses, are provided in this appendix to Chapter 7.

A Failure Modes and Effects Analysis (FMEA) of the Essential Multiplexing System is provided in Appendix 15B.

[*The following two Items must be addressed when any change is made in the commitments of the EMS and SSLC Design:*

*(1) Table 10 of DCD/Introduction identifies the commitments for EMS performance specifications and architecture which, if changed, requires NRC Staff review and approval prior to implementation. The applicable portions of the Tier 2 sections and tables, identified on Table 10 of DCD/Introduction for this restriction, are italicized on the sections and tables themselves.*

(2) *Table 11 of DCD/Introduction identifies the commitments for SSLC hardware and software qualification which, if changed, requires NRC Staff review and approval prior to implemtentation. The applicable portions of the Tier 2 sections and tables, identified on Table 11 of DCD/Introduction for this restricition, are italicized on the sections and tables themselves.*]*

## *7A.2 [Multiplexing Systems*

***NRC Request (1)—****Provide a complete list of components (pumps, valves, etc.) whose actuation, interlock, or status indication is dependent on the proper operation of each Class 1E multiplexer.*

* See Section 3.5 of DCD/Introduction.

***Response (1)—****The list is provided as Table 7A-1. It was obtained by extraction from the multiplexer I/O database which reflects information available on the system P&ID and IBD drawings.*

***NRC Request (2)—****For the components cited above, describe the means of remote or local control (other than by cutting wires or jumpering) that may be employed should the multiplexer fails.*

***Response (2)—****All Class-1E multiplex hardware is designed to meet the single-failure criteria. Systems which employ such hardware have redundant channels such that no single failure of any MUX unit could jeopardize any safety system action. In addition, local control is provided, via the Remote Shutdown System, to bring the reactor to shutdown conditions in event of multiple safety system failures or evacuation of the control room. The Remote Shutdown System is hard-wired and therefore provides diversity to the MUX interfaces.*

***NRC Request (3)—****Describe the multiplexer pre-operational test program.*

***Response (3)—****The pre-operational test program will test the multiplexers concurrently with instrumentation and control functional loop checks. As each input to a remote multiplexing unit (RMU) is simulated using a suitable input device, the required outputs shall be verified correct. In this manner, all hardware and software are confirmed concurrently.*

*Equipment verifications of the individual multiplexing units are performed at the factory and typically include detailed component level tests which require special test apparatus and technical expertise. Any malfunctioning not found during factory testing will be detected during pre-operational tests of instrument loops.*

*Testing shall include instrument loop checks, calibration verification tests and response time verification tests as described in ANSI/IEEE-338. If possible, the entire instrument loop shall be tested from sensor to output device(s). Otherwise, suitable input devices shall be used to simulate process inputs and the system outputs verified to be acceptable.*

*In addition to the testing described above, tests shall be developed to verify system redundancy and electrical independence.*

***NRC Request (4)—****Describe the test and/or hardware features employed to demonstrate fault tolerance to electromagnetic interference.*

***Response (4)—****One major deterrence to electromagnetic interference (EMI) in the multiplexing system is the use of fiber optic data links as the transmission medium. Optical fiber, being a non-electrical medium, has the inherent properties of immunity to electrical noise (EMI, RFI, and lightning), point-to-point electrical isolation, and the absence of conventional transmission line effects. Fiber optic multiplexing is also unaffected by the radiated noise from high voltage conductors, by high frequency motor control drives, and by transient switching pulses from electromagnetic contactors or other switching devices.*

*However, the electrical-to-optical interface at the transmitting and receiving ends must still be addressed to ensure complete immunity to EMI. The control equipment containing the electrical circuitry use standard techniques for shielding, grounding, and filtering and are mounted in grounded equipment panels provided with separate instrument ground buses. Panel location, particularly in local areas, is carefully chosen to minimize noise effects from adjacent sources. The use of fiber optic cables ensures that current-carrying ground loops will not exist between the control room and local areas.*

*The use of redundancy provides the other major deterrence to EMI effects. The safety-related multiplexing system uses redundant optical channels within each separated electrical division. The systems are independent and will run asynchronously with respect to each other with no communication between divisions. However, data communication and transfer is synchronized within each division itself. This arrangement provides fault tolerance to EMI or other noise occurring in isolated locations.*

*During normal operation, multiplexing system performance will be monitored by online tests such as parity checks, data checks (boundary and range), and transmission timing. If response time requirements permit, error correcting algorithms may be applied to mask noise effects. Periodic surveillance using offline tests such as bit error rate will be used to verify overall system integrity.*

*As part of the pre-operational test program [see Request (3)], the system will be subjected to EMI testing. EMI and RFI test measurements will be developed using the guidelines described in ANSI/IEEE-C63.12, "American National Standard for Electromagnetic Compatibility Limits—Recommended Practice." For testing susceptibility to noise generation from portable radio transceivers, tests will be developed from ANSI/IEEE-C37.90.2, "IEEE Trial-Use Standard, Withstand Capability of Relay Systems to Radiated Electromagnetic Interference from Transceivers." Section 5.5.3 of this standard describes tests for digital equipment using clocked logic circuits.*

*With the system connected, each multiplexing unit (one at a time) will be required to demonstrate immunity to the defined conducted and radiated tests. Units shall also comply with standard surge withstand capability tests, as follows:*

*(a) ANSI/IEEE-C62.41—"Guide for Surge Voltages in Low-Voltage AC Power Circuits."*

*(b) ANSI/IEEE-C62.45—"Guide on Surge Testing for Equipment Connected to Low-Voltage AC Power Circuits."*

*The interconnecting fiber optic links of the multiplexing system and SSLC are not subject to EMI effects.*

*For design guidance and additional test development guidance, the following military standards shall be used:*

*(a) MIL-STD-461C—"Electromagnetic Emission and Susceptibility Requirements for the Control of Electromagnetic Interference."*

*(b) MIL-STD-462—"Measurement of Electromagnetic Interference Characteristics."*

*Due to the comprehensive nature of these documents, their applicability to ground, airborne, and shipboard equipment, and the differences in requirements for the Army, Navy and Air Force, the use of these standards shall be limited to the susceptibility requirements and limits for class A3 equipment and subsystems (ground, fixed). Within these limits, the guidelines for Army procurements only shall be used. Tests for transmitting and receiving equipment, power generators, and special purpose military devices are not applicable.*

**[*To facilitate achieving EMC compliance, system and equipment grounding and shielding practices will follow the guidance of the standards listed below:*

***(a) IEEE Std. 518, "Guide for the Installation of Electrical Equipemnt to Minimize Electrical Noise Inputs to Controllers from External Sources."***

***(b) IEEE Std. 1050, "Guide for Instrumentation and Control Equipment Grounding in Generating Stations."*]***

***NRC Request (5)—****Describe the interconnection, if any, of any Class 1E multiplexer to non-Class 1E devices such as the plant computer.*

***Response (5)—****The interconnection of Class 1E multiplexers to non-Class 1E devices is done using fiber optic cable. The fiber optic cable will provide the necessary isolation.*

*The plant process computer is connected to a buffer module (memory storage module). Information is stored in this module by the 1E MUX units for access by the process computer, thus preventing any interruption by the Non 1E process computer on the 1E MUX units.*

***NRC Request (6)—****Describe the online test and/or diagnostic features that may be employed, including any operator alarms/indicators and their locations.*

***Response (6)—****The EMS self-test system relies on the Safety System Logic and Control (SSLC) test control unit, though it has also its own local self-test system. Local self-test in each EMS unit continues to provide diagnostic readout even if the test control unit fails.*

*A continuously operating self-test system checks all data transmission and provides operators with fault information and fault location through dedicated alarms and computer output. The self-test system operation or its failure cannot harm the operation of the safety systems.*

*Figure 7A-1 shows the general concept of the EMS interface with the test control unit. The online test and diagnostic features including operator alarms and location are detailed as follows:*

* See Section 7A.1(2) and 7A.1(1).

- *Self-test locates a fault down to the processing module level and provides positive local identification of the failed device.*
- *A periodic, automatic test feature verifies proper operation of the EMS.*
- *Detection of fatal (affects signal transmission) and non-fatal (does not affect signal transmission) errors is annunciated and relayed to the computer. Operators are informed on the type of malfunction and its location.*
- *Local self-test is continuous. System end-to-end test is initiated in one division at a time by communication between test units in each division.*
- *The logic returns to its original state after the test sequence is completed. Indications of test status (normal or in-test) and results (pass, fail) is provided.*
- *The test function does not degrade system reliability. The test circuitry is physically and electrically separated and isolated from the functional circuitry insofar as possible. Testing will not cause actuation of the driven equipment.*
- *Automatic initiation signals from plant sensors override an automatic test sequence and perform the required safety function.*
- *Failure of the test control unit does not affect the safety system functional logic.*

***NRC Request (7)—****Describe the multiplexer power sources.*

***Response (7)—****The multiplexer system receives its power from the four-divisional battery 125 VDC buses. These are discussed in Subsection 8.3.2 and illustrated in Figure 8.3-4.*

***NRC Request (8)—****Describe the dynamic response of the multiplexers to momentary interruptions of AC power.*

***Response (8)—****Each of the four divisions of the multiplexer system is fed by the corresponding division of the 125 VDC battery. Therefore, the multiplexer system will not be affected by momentary interruption to the AC power. Extended losses of power in any division would not affect operations of safety functions because of multiplicity of divisional power (Figure 8.3-3).*

*If EMS power is interrupted and subsequently restored, then the EMS unit reinitializes automatically and the system reconfigures to accept the signal transmission.*

***NRC Request (9)—****Describe the applicability of the plant Technical Specifications to multiplexer operability.*

***Response (9)—****The applicability of the plant Technical Specifications to the four-division multiplexer operability will be a section in the specifications that will include limiting condition for operation, and surveillance requirements.*

*The limiting condition is expected to be similar to that for a loss of a divisional electrical power supply.*

***NRC Request (10)—****Describe the hardware architecture of all multiplexer units.*

***Response (10)—****The multiplexer units are of two types:*

*(1) Remote Multiplexing Units (RMU)*

*(2) Control Room Multiplexing Units (CMU)*

*System Configuration*

*In each protection division, RMUs are located in local plant areas to acquire sensor data and transmit it to the control room for processing. The RMUs also receive processed signals from the control room for command of safety system actuators. CMUs are located in the control room to transmit and receive data for the logic processing units of the safety protection system (RPS and ESF). Response time constraints may dictate RPS outputs be hardwired (not multiplexed) to the load drivers.*

*All interconnections are fiber optic data links. Within each division, the system uses redundant links (either in a hot standby configuration or a bi-directional, reconfigurable arrangement) for greater reliability.*

*The safety-related multiplexing systems in each division are separated and independent.*

*Hardware Configuration*

*(1) RMU*

*(a) Microprocessor-based, bus-oriented architecture with control program in ROM (i.e., firmware).*

*(b) Modular design: Plug-in modules or circuit boards with distinct functions on separate modules (CPU, memory, I/O). Redundant low voltage power supplies are used for greater reliability.*

*(c) Input modules acquire safety-related analog and digital data from process transmitters and equipment status contact closures, respectively. Analog input modules perform signal conditioning and A/D conversion. Digital input modules perform signal conditioning (filtering, voltage level conversion).*

*(d) Output modules transmit processed control signals to equipment actuator circuits (output signals may be contact closures or voltage levels to drive relays or solid-state load drivers).*

*(e) Communications interface modules format and transmit input signals as serial multiplexed words via fiber optic data links from local areas to the control room multiplexing units. These modules also receive processed signals from the control room and demultiplex and prepare output signals for interfacing to actuators.*

*(f) CPU and memory modules coordinate I/O and communication functions and perform peripheral tasks such as self-test and calibration.*

*(g) Front panel interface (isolated from safety-critical signal path) permits technician access to calibration and diagnostic functions.*

*(2) CMU*

*(a) Same as RMU.*

*(b) Same as RMU.*

*(c) Input modules: None.*

*(d) Output modules: None.*

*(e) Communications interface modules acquire serial data from control room logic processing units. The data is formatted and inserted via a fiber optic interface into the multiplexed data stream out to the RMUs. The modules also receive multiplexed serial data from the RMUs, demultiplex the data, and transmit it to the control room logic processing units via an optical serial link.*

*(f) Same as RMU.*

*(g) Same as RMU.*

**[*The development of the essential multiplexing as a deterministic, dual redundant, fiber optic ring structure shall follow the Fiber Distributed Data Interface (FDDI) protocol as described in the following American National Standards Insitute (ANSI) reference documents:***

***(a) ANSI X3.166, "Fiber Distribution Data Interface (FDDI) - Physical Layer Medium Dependent (PMD)."***

***(b) ANSI X3.148, :Fiber Distributed Data Interface (FDDI) - Token Ring Physical Layer Protocol (PHY)."***

***(c) ANSI X3.139, "Fiber Distributed Data Interface (FDDI) - Token Ring Media Access Control (MAC)."***

(d) ***ANSI X3T9.5/84-49, "FDDI Station Management (SMT)," Prelimiary Draft.*]***

*For portions of the safety systems where the data throughput requirement is less than 5M bit/s, IEEE-802.5, Token Ring Access Method and Physical Layer Specifications, may be implemented as an alternative, using either coaxial, twisted-pair or fiber optic cable as the transmission medium. Both networks conform to ISO 7498, Open Systems Interconnection—Basic Reference Model, as the Data Link Layer and Physical Layer. For the Data Link Layer, IEEE-802.2, Standard for Local Area Networks: Logical Link Control, shall be used with either network to define the protocols necessary to move data to the higher levels of the ISO model.*

*Communications protocols used for data transmission in other parts of the safety system and for transferring data to the non-safety systems shall also conform to ISO 7498.*

---

* See Sections 7A.1(2) and 7A.1(1).

***NRC Request (11)—****Describe the "firmware" architecture.*

***Response (11)—****The "firmware" (software contained in ROM) architecture depends upon knowledge of a specific hardware/software combination for the multiplexer units. Since Tier 2 is to be independent of specific vendor's hardware and is, instead, based upon system level requirements, the exact configuration of software for the multiplexer units is not specified. However, software development will follow a process consistent with the safety-related nature of the multiplexing system.*

*The software must also support the following characteristics of the multiplexing system:*

*(1) The multiplexing system is a real-time control application configured as a fiber optic local area network.*

*(2) Because time response for some functions is critical to safety, system timing must be deterministic and not event-driven. A typical industry standard communications protocol that is likely to be used is FDDI (Fiber Distributed Data Interface), a token-passing, counterrotating ring structure with data rates to 100M bit/s. Hardware communications interfaces to this protocol are available, thus reducing the need for special software development.*

*(3) The safety-critical system functions are analog and digital data acquisition, signal formatting, signal transmission, demultiplexing, and control signal outputs to actuators. Peripheral functions are self-test features and system calibration (e.g., adjustment of A/D converters).*

*(4) During system initialization or shutdown and after loss of power, control outputs to actuators must fail to a safe state (fail safe or fail-as-is, as appropriate for the affected safety system). System restart shall not cause inadvertent trip or initiation of safety-related equipment (i.e., system output shall depend only on sensed plant inputs).*

*(5) The system must be fault-tolerant to support the single-failure criterion. Multi-division duplication of the system will provide this feature; however, within each division, the system will also be redundant for high availability. Thus, the software must perform failure detection and automatic switchover or reconfiguration in case of failure of one multiplexer channel.*

*High quality software is the most critical aspect of microprocessor-based designs for safety systems. The software must be of easily proven reliability so as not to degrade the reliability and availability of the overall system. When installed as "firmware", the software should become, in effect, another high quality hardware component of the control equipment, especially, since the program in ROM is protected from being changed by external sources.*

*Software development will, in general, follow Regulatory Guide 1.152, which endorses ANSI/IEEE ANS-7-4.3.2. These documents emphasize an orderly, structured, development approach and the use of independent verification and validation to provide traceable confirmation of the design. Validation must verify a predictable and safe response to abnormal as well as normal test cases. A software-based design must also support the testability, calibration and bypass requirements of IEEE-279.*

*To meet the above requirements, the software will be developed as a structured set of simple modules. Each module will perform a prescribed task that can be independently verified and tested. Modules shall have one entry and one exit point. The software requirements specification and design specification will define structures of external files used and interfaces with other programs. In place of a formal operating system, an "executive" control program or real-time kernel will monitor, schedule, and coordinate the linking and execution of the modules. The integration of the modules into the control program will be another activity to be independently verified and validated.*

*The overall program structure will be a hierarchy of tasks. Separate modules will be created for safety-critical tasks, calibration functions, and self-test functions, with self-test running in the background at the lowest priority. Highest priority functions will always run to completion. The use of interrupts will be minimized to prevent interference with scheduled tasks.*

*On detection of faults, retry or rollback to the last known correct state will be permitted within system time constraints. If the fault is permanent and potentially unsafe, the system shall recover (or fail) to a safe state and the operator shall be alerted. The redundant multiplexing channels shall be repairable online if one channel fails. All processor memory not used for or by the operational program shall be initialized to a pattern that will cause the system to revert to a safe state if executed.*

*The software shall permit online calibration and testing with the outputs to the safety systems bypassed.*

*The software design shall prevent unauthorized access or modification.*

*Software development to achieve program operation as described above and to document and verify this operation shall conform to the following standards:*

***(1) [IEEE-828, "IEEE Standard for Software Configuration Management Plans"***

***(2) IEEE-829, "IEEE Standard for Software Test Documentation"***

***(3) IEEE-830, "IEEE Standard for Software Requirements Specifications"***

***(4) IEEE-1012, "IEEE Standard for Software Verification and Validation Plans"***

***(5) IEEE-1042, IEEE Guide to Software Configuration Managenent]**** |

***NRC Request (12)**—Provide an explicit discussion of how the systems conform to the provisions of IEEE-279, Section 4.17.*

***Response (12)**—The multiplexing system for safety systems only acquire data from plant sensors (pressure, level, flow, etc.) and equipment status contact closures (open, close, start, stop, etc.) that provide automatic trip or initiation functions for RPS and ESF equipment.*

* See Sections 7A.1(2) and 7A.1(1).

*Manual initiation inputs for protective action are implemented by direct, hardwired or optical connections to the safety system logic (e.g., ECCS, containment isolation). Initiation outputs for ECCS and isolation functions (except MSIV) are multiplexed to the actuators. Manual scram (reactor trip) is provided by breaking the power source to the scram pilot valve solenoids external to the multiplexing system and safety system logic. Manual reactor trip and manual MSIV closure in each division are available even with multiplexing system failure, since these outputs are not multiplexed to the actuators.*

*However, because the multiplexing system design is fault tolerant (replicated in four divisions and redundant within each division) [see the responses to Requests (4), (10), and (11)], a single failure will not degrade data communications in any division.*

*Therefore, the requirements of IEEE-279, Section 4.17, are satisfied, since a single failure will not prevent initiation of protective action by manual or automatic means.*

*The last sentence of Section 4.17 states that "manual initiation should depend upon the operation of a minimum of equipment". The first paragraph has shown that reactor trip and MSIV initiation do not depend at all on the multiplexing system. ECCS initiation and isolation initiation other than MSIV do not depend on multiplexing for sending inputs to the logic and depend on the operation of only one channel of multiplexing in each division to send outputs to actuators.*

***NRC Request (13)**—Provide an explicit discussion of how the systems conform to IEEE 279, Paragraph 4.7.2, as supplemented by Regulatory Guide 1.75 and IEEE 384.*

***Response (13)**—The safety-related multiplexing system, which is part of the protection system, has no direct interaction with the control systems. Sensor and equipment status data are multiplexed only to protection system logic. However, two signals are sent from the protection system logic to the Recirculation Flow Control System: Reactor Water Level 2 Trip and Recirculation Pump Trip. The signals are transmitted via fiber optic data links, which are not part of the multiplexing system. An isolating buffer (gateway) transfers these signals to the non-safety-related multiplexing network of the control systems.*

*Fiber optic transmission lines are not subject to credible electrical faults such as short-circuit loading, hot shorts, grounds or application of high AC or DC voltages. Adjacent cables are not subject to induced fault currents or to being shorted together. The effects of cable damage are restricted to signal loss or data corruption at the receiving equipment. Cables and control equipment of different systems or assigned to different divisions are kept separated only to prevent simultaneous physical damage.*

*Thus, the multiplexing system conforms to IEEE-279, paragraph 4.7.2, in that no credible failure at the output of an isolation device can "prevent the protection system channel from meeting minimum performance requirements specified in the design bases."*

*To meet the requirements of IEEE-384 and Regulatory Guide 1.75, the protective covering of the fiber optic cables are flame retardant. The cables are passed through physical, safety class barriers, where necessary, for separation of Class 1E circuits and equipment from other Class 1E equipment or from non-Class 1E equipment. The fiber optic multiplexing network is independent in each protection division and does not transmit or receive data between divisions. However, the multiplexing equipment is kept physically separate to minimize the effects of design basis events.*

***NRC Request (14)**—Provide confirmation that system level failures of any multiplexer system detected by automated diagnostic techniques are indicated to the operators consistent with Regulatory Guide 1.47. (i.e., bypass and inoperable status indication)*

***Response (14)**—Each safety-related multiplexing system contains online self-diagnostics implemented in software and hardware that will continuously monitor system performance. Within each control station, the following typical parameters are monitored: (1) status of the CPU, (2) parity checks, (3) data plausibility checks, (4) watchdog timer status, (5) voltage levels in control unit circuitry, (6) memory (RAM and ROM) checks, and (7) data range and bounds checks. Hardware is provided prior to transmission and following reception to detect transmission errors at the Remote Multiplexing Units and the Control Room Multiplexing Units. Self-test will indicate faults to the module board replacement level.*

*Each multiplexing system has dual channels for fault tolerance and is provided with automatic reconfiguration and restart capability. A detected fault is automatically annunciated to the operator at both the system and individual control station level. If one transmission loop is completely out of service, that will also be annunciated. Total shutdown of a multiplexing system is indicated by a separate alarm; however, individual control stations are repairable online without taking the entire system down.*

*The above actions indicate conformance to Regulation Guide 1.47, Section C.1 (Automatic system level indication of bypass or deliberately induced inoperability).*

*After repair, the system automatically re-initializes to normal status when power is restored to any unit and automatically resets any alarms. Power loss to any control station is separately monitored and annunciated to aid in troubleshooting and to alert the operator when power is deliberately removed from a unit when being serviced. Power loss will cause the fault or out-of-service alarms described previously to activate. This indicates conformance to Regulation Guide 1.47, Section C.2 [Automatic activation of indicating system of C.1 when auxiliary or supporting system (in this case, power source) is bypassed or deliberately rendered inoperable].*

*Bypassed or inoperable status of any one multiplexing system can not render inoperable any redundant portion of the protection system. Each multiplexing system is independent in each division. Inoperable status in one division will cause the appropriate safe-state trips in that division, but the other divisions will continue to operate normally. Faults in another division simultaneously will indicate according to the previous discussion. The resulting safe-state trips will*

*result in the required protective action. Thus, the requirements of Regulation Guide 1.47, Section C.3, are satisfied.*

*During periodic surveillance, the system-level out-of-service indicators can be tested manually. This satisfies the requirement of Regulation Guide 1.47, Section C.4.*

***NRC Request (15)**—Provide an explicit discussion of the susceptibility of the multiplexer systems to electromagnetic interference.*

***Response (15)**—Each control station of the multiplexer system, either in the control room or in local areas is electrically powered and contains solid-state logic and, therefore, is potentially susceptible to the effects of EMI. However, the effects on the overall network are reduced because of the dual, fiber optic, data transmission network that is used between stations. Fiber optics are not subject to induced electrical currents, eliminate ground loops, and also do not radiate electrical noise. Thus, the isolated and distributed nature of the system, which is also replicated in four divisions, tends to reduce EMI effects.*

*Response (4) indicates several common techniques (shielding, grounding, etc.) used to minimize EMI in the electrical control circuitry. Proper physical placement, especially for the Remote Multiplexing Units, is essential to eliminate interference from high current or high voltage switching devices.*

*Data checking software at the RMUs and in the control room at the Control Room Multiplexing Units monitors data transmission to ensure that faults do not propagate into the safety protection logic. Bad data transmission will cause a system alarm and, possibly, a system shutdown if the fault does not clear within defined time constraints.*

*Response (4) also discusses various tests that the system will undergo to demonstrate immunity to EMI.*

## 7A.3 Electrical Isolators

***NRC Request (1)**—For each type of device used to accomplish electrical isolation, provide a description of the testing to be performed to demonstrate that the device is acceptable for its application(s). Describe the test configuration and how the maximum credible faults applied to the devices will be included in the test instructions.*

***Response (1)**—This response is limited to fiber optic data links, which are the only type of isolation device used for electrical isolation of logic level and analog signals between protection divisions and from protection divisions to non-safety-related equipment.*

*Testing is of two types:*

*(1) Optical characteristics*

*(2) Signal transmission capability*

*Optical characteristics are checked by an optical power meter and a hand-held light source to determine the optical loss from one end of the fiber optic cable to the other. In an operational system, an optical time domain reflectometer measures and displays optical loss along any continuous optical fiber path. Any abrupt disruption in the optical path such as a splice or connector is seen as a blip on the display. This technique is especially useful for troubleshooting long runs of cable such as in the multiplexing system. Cable terminations are visually inspected under magnification to determine if cracks and flaws have appeared in the optical fiber surfaces within the connector.*

*Transmission characteristics are tested by bit generation. This test method determines bit error rate by generating a random stream of bits at the transmitter and verifying them at the receiver to determine the reliability of the fiber optics. Data rate is set at the maximum throughput required by the system. Proper transfer of analog signals is determined by analog-to-digital conversion of test signals at the transmitting end, and monitoring of the digital-to-analog conversion at the receiving end for linearity over the full scale range. Frequency of the test signals is set at the maximum required by the system.*

*Maximum credible electrical faults applied at the outputs of isolation devices do not apply to fiber optic systems. The maximum credible fault is cable breakage causing loss of signal transmission. Faults cannot cause propagation of electrical voltages and currents into other electrical circuitry at the transmitting or receiving ends. Conversely, electrical faults originating at the input to the fiber optic transmitter can only damage the local circuitry and cause loss or corruption of data transmission; damaging voltages and currents will not propagate to the receiving end.*

***NRC Request (2)**—Identify the data that will be used to verify that the maximum credible faults applied during the test are the maximum voltage/current to which the device could be exposed, and to define how the maximum voltage/current is determined.*

***Response (2)**—The response to Request (1) established that electrical faults are not credible at the output of a fiber optic isolating device. Therefore, Request (2) is not relevant.*

***NRC Request (3)**—Identify the data that will be used to verify that the maximum credible fault is applied to the output of the device in the transverse mode (between signal and return) and other faults are considered (i.e., open and short circuits).*

***Response (3)**—The response to Request (1) established that electrical faults are not credible at the output of a fiber optic isolating device. Open and short circuits of the fiber optic cable have no electrical effect on the input side electrical circuitry.*

***NRC Request (4)**—Define the pass/fail acceptance criteria for each type of device.*

***Response (4)**—Since electrical faults at the outputs are not credible, acceptance tests for fiber optic isolation devices need only verify optical characteristics and signal transmission characteristics as defined in Response (1).*

***NRC Request (5)****—Provide a commitment that the isolation devices will comply with all environmental qualification and seismic qualification requirements.*

***Response (5)****—Fiber optic isolation devices are expected to have less difficulty than previous isolation devices in complying with all qualification requirements due to their small size, low mass, and simple electronic interfaces. The basic materials and components, except for the fiber optic cable itself, are the same as those used in existing, qualified isolation devices.*

*A major advantage of fiber optics is that signals can be transmitted long distances and around curves through the isolating medium; thus, the physical, safety-class barrier required for separation of Class 1E devices may be provided by just the cable length if the protective covering and any fill materials of the cable are made properly flame-retardant. For short distances, the fiber optic cable can be fed through a standard safety class structure.*

*Details of the type of cable, transmitter, and receiver combinations that will provide optimum compliance with qualification requirements must await the guidance to be developed by the NRC staff/EG&G studies (see Section 4).*

***NRC Request (6)****—Describe the measures taken to protect the safety systems from electrical interference (i.e., electrostatic coupling, EMI, common mode, and crosstalk) that may be generated.*

***Response (6)****—Previous responses have described the specific measures that are employed to minimize electrical interference. Fiber optic isolating devices do not require metallic shielding and are immune from electrostatic coupling, EMI, common-mode effects, and crosstalk along their cable length; they also do not radiate electrical interference. The electrical circuitry used to transmit and receive the optical signals is susceptible to electrical interference in the same manner as other circuitry, but the isolating effects of the fiber optic cable will reduce propagation of interference. The local effects of EMI and other electrical noise are handled by standard filtering, shielding, and grounding techniques.*

*See Reponse (4) of Section 7A.2 for tests that will be performed to verify the effectiveness of EMI preventive measures for safety systems. Additional tests to determine the susceptibility of safety system control equipment to electrostatic discharges shall be established using the test procedures included in IEC Publication 801-2, Electromagnetic Compatibility for Industrial-Process Measurement and Control Equipment, Part 2: Electrostatic Discharge Requirements. The test procedures of Paragraph 8 of this document shall be performed up to and including Severity Level 4, as defined in the document.*

***NRC Request (7)****—Provide information to verify that the Class 1E isolation devices are powered from a Class 1E power source(s).*

***Response (7)****—When using fiber optic devices as Class 1E isolation devices, only the input side of the transmitting device and output side of the receiving device use electrical power. The low voltage*

*power supplies for these devices use the same power source as the logic that drives the isolating device. For ABWR safety systems, this power is:*

*(1) Divisional 120V Vital AC (UPS)—For Reactor Protection System (RPS) logic and Main Steam Isolation Valve (MSIV) logic.*

*(2) 125V Plant DC Power Supply—For ECCS logic and Leak Detection and Isolation System (LDS) logic.*

***NRC Request (8)**—Provide a comparison of the design with the guidance in NUREG/CR-3453/EGG-2444, "Electronic Isolators Used in Safety Systems of U.S. Nuclear Power Plants," March 1986.*

***Response (8)**—The isolating devices used for the ABWR are similar to the Group 1 types referred to in the NUREG. They are of the long fiber optic cable design, so transmitting and receiving ends are separated by a significant distance (typically several feet to several hundred feet). These types of designs had the best isolating characteristics of the various isolators compared in the NUREG study.*

*Typically, the electrical-to-optical interfaces are part of the general logic processing equipment within a channel and do not reside in separate isolator units. The fiber optic interfaces receive the protection from EMI and surge currents designed into the logic equipment (for example, power supply decoupling, shielding, filtering, single-point signal common connection to chassis ground, and chassis ground connection to panel ground bus). The equipment will undergo EMI and surge testing to the standards identified in the NUREG or equivalent.*

*The results of the NUREG tests show that the fiber optic type of isolators exhibited no or very little effects from the major fault and lightning surge tests. Only surge and EMI tests applied to the isolator power supplies caused damage to the isolator input side, mainly because of the output and input supplies sharing a common, commercial AC power line. However, as noted in the NUREG BWRs do not directly use a commercial power source. For the ABWR, RPS and ESF functions are supplied from different plant power sources (120V Vital AC and 125 VDC, respectively). The low voltage DC supplies fed from these sources are highly regulated and filtered. Thus, isolator circuitry is isolated from most power source transients.*

***NRC Request (9)**—Provide a comparison of the design with the guidance in draft Regulatory Guide EE502-4, "Criteria for Electrical Isolation Devices Used in Safety Systems for Nuclear Power Plants".*

***Response (9)**—(Draft RG EE502-4 was withdrawn by the NRC.)*]*

* See Section 7A.1(1).

## 7A.4 Fiber Optic Cable

The staff is working with EG&G to develop comprehensive guidance on this subject. The guidance will be based on the existing IEEE cable standards, such as IEEE-323 and IEEE-384, on the ANSI standards for fiber optic cables (list provided), and the results of the EG&G work.

## *7A.5 [Programmable Digital Computer Software**

***NRC Request**—Provide a comparison of the design with the following:*

***(1) [ANSI/IEEE-ANS-7.4.3.2, "Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations." ]†***

*(2) Regulatory Guide 1.152, "Criteria for Programmable Digital Computer System Software in Safety-Related Systems of Nuclear Power Plants," November 1985*

*(3) NUREG-0308, "Safety Evaluation Report—Arkansas Nuclear 1, Unit 2," November 1977*

*(4) NUREG-0493, "A Defense-in-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System," May 1985*

*(5) NUREG-0491, "Safety Evaluation Report of RESAR-414," February 1979*

## *7A.6 Programmable Digital Computer Hardware ‡*

***NRC Request**—Provide a comparison of the design with the following:*

*(1) IEEE-603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations"*

*(2) NUREG-0308, "Safety Evaluation Report— Arkansas Nuclear 1, Unit 2," November 1977*

*(3) Regulatory Guide 1.153, "Criteria for Power, Instrumentation and Control Portions of Safety Systems"*

*(4) NUREG-0493, "A Defense-in-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System," May 1985*

---

* Responses to Sections 7A.5 and 7A.6 above are grouped in various combinations, as appropriate, in Subsection 7A.7

† See section 7A.1(2) and 7A.1(1).

‡ Responses to Sections 7A.5 and 7A.6 above are grouped in various combinations, as appropriate, in Subsection 7A.7

(5) NUREG-0491, "Safety Evaluation Report of RESAR-414," February 1979

## 7A.7 Responses to Subsections 7A.5 & 7A.6; Computer Hardware and Software

### Items 7A.5(1) and 7A.5(2)

*Criteria and guidelines stated in ANSI/IEEE-ANS-7.4.3.2, as endorsed by Regulatory Guide 1.152, have been used as a basis for design procedures established for programmable digital equipment.*

*All programmable digital equipment utilized for safety-related functions are qualified in accordance with safety criteria and with the safety system design basis with which they interface.*

*Self-test or self-diagnostic features of this equipment, whether implemented in hardware or software, are considered an integral part of the design, and, as such, are qualified to Class 1E standards.*

*A structured, engineered approach to the development of both hardware and software is implemented to assure that the design proceeds along the lines of the requirement specifications and has traceable documentation.*

*Verification and validation (V&V) includes the establishment of test and evaluation criteria, the development of test and evaluation procedures, the testing of the integrated hardware and software, and the installation of the hardware and software in the field.*

*In accordance with the step-by-step verification process, design reviews are performed at the system functional and performance requirements specification/task analysis and allocation of functions level, the hardware design and the software design level, the test and evaluation criteria and procedures level, and the personnel requirements and operating/maintenance plan level. Such reviews are conducted by knowledgeable and experienced system engineers, software engineers, hardware engineers, etc., who are not directly responsible for the design, but who may be from the same organization.*

*Figure 7A-2 illustrates the structure utilized for ABWR control and instrumentation system design which incorporates subject guidelines.*

### Items 7A.5(3) and 7A.6(2)

*NUREG-0308, "Safety Evaluation Report—Arkansas Nuclear 1, Unit 2", was reviewed and generally found to be not applicable to the BWR/ABWR reactor design philosophy.*

*The NUREG discusses a "Core Protection Calculator System (CPCS)" which is designed to provide reactor protection for two conditions: (1) low local departure from nucleate boiling ratio (DNBR), and (2) high local linear power density.*

*For condition (1), "DNBR" is associated with PWRs and is not applicable to BWRs. For condition (2), power density is determined via the Neutron Monitoring System (NMS), similar to methods used in operating BWRs (see Subsection 7.6.1.1 for discussion of the NMS).*

*The ABWR design of the Reactor Protection System utilizes microprocessor technology for logic decisions based on analog input from various sensors. This philosophy is much the same as that of GESSAR II and the Clinton BWR, except in those designs, solid-state CMOS accepted digital signals from analog trip modules (ATM). In the ABWR design, the microprocessors perform the functions of both the CMOS and the ATM.*

*The important distinction is that the ABWR uses a modern form of digital computer device (i.e., microprocessors) for the same reasons relays and solid-state devices were used in earlier designs (i.e., making simple logic decisions); not for making complex calculations for which protective action is dependent.*

### *Items 7A.5(4) and 7A.6(4)*

*The guidelines of NUREG-O493 have been used to perform analysis of several possible different configurations of the Safety System Logic and Control (SSLC) network. Analyses have been performed at the system design level to assure adequate defense-in-depth and/or diversity principles were incorporated at acceptable cost. It is recognized that such requirements are in addition to positions on safety-related protection systems (such as the single failure criterion) taken previously in other Regulatory Guides.*

*In order to reduce plant construction costs and simplify maintenance operation, the ABWR protection sytems are designed with a "shared sensors" concept. The SSLC is the central processing mechanism and produces logic decisions for both RPS and ESF safety system functions. Redundancy and "single failure" requirements are enhanced by a full four-division modular design using two-out-of-four voting logic on inputs derived from LOCA signals which consist of diverse parameters (i.e., reactor low level and high drywell pressure). Many additional signals are provided, in groups of four or more, to initiate RPS scram (Table 7.2-2).*

*With its inherent advantages, it is also recognized that such design integration (i.e., shared sensors) theoretically escalates the effects of potential common-mode failures (CMF). Therefore, SSLC System architecture is designed to provide maximum separation of system functions by using separate digital trip modules (DTMs) and trip logic units (TLUs) for RPS/MSIV logic processing and for LDS/ECCS logic processing within each of the four essential power divisions. Thus, setpoint comparisons within individual DTMs are associated with logically separate initiation tasks.*

*Sensor signals are sent to each DTM on separate or redundant data links such that distribution of DTM functions results in minimum interdependence between echelons of defense. For reactor level sensing, the RPS scram function utilizes narrow-range transmitters while the ECCS functions utilize the wide-range transmitters. The diverse high drywell signals are shared within the two-out-of-four voting logic. In addition, all automatic protective functions are backed up by manual controls. These concepts are illustrated in Figure 7A-1.*

*As a general rule, shared sensors for protection systems are not used for control systems (i.e., feedwater, recirc, etc.). However, the end-of-cycle (EOC) recirc pump trip signals originate from the same turbine stop valve closure or turbine control valve fast closure sensors which contribute to*

*scram. These are Class 1E sensors, but they are not shared with other protection systems and the interface with the recirc system is naturally isolated via fiber-optic cable.*

*Another use for some of the protection shared signals involves the ATWS trip which activates the Fine Motion Control Rod Drive (FMCRD) run-in and alternate rod insertion (ARI) as diverse backup to hydraulic scram. However, this Class-1E-to-non-Class-1E isolated interface is a special case for mitigation of ATWS and is not a control system interface.*

*The ABWR demonstrates strong multi-system diversity in its capability to shut down and cool the reactor core. There are four distinct systems for controlling reactivity and four distinct systems for cooling the core.*

*Reactor Shutdown Systems*

*(1) The RPS "failsafe" (i.e., scram on loss of power or data communications) hydraulic scram (Subsection 7.2.1.1.4).*

*(2) The ATWS-mitigating DC-power-actuated air header dump valves (alternate rod insertion [ARI]) scram (Subsection 7.2.1.1.4.5).*

*(3) The ATWS-mitigating rod run-in function utilizing fine-motion control rod drive (Subsection 7.7.1.2.2).*

*(4) The Standby Liquid Control System (Subsection 7.4.1.2).*

*Reactor Core Cooling Systems*

*(1) The Feedwater Control System (Subsection 7.7.1.4).*

*(2) The High Pressure Core Flooder System (Subsection 7.3.1.1.1.1).*

*(3) The turbine-driven Reactor Core Isolation Cooling System (Subsection 7.3.1.1.1.3).*

*(4) The low pressure flooder mode of RHR (Subsection 7.3.1.1.4).*

*The Remote Shutdown System (RSS) also provides an independent means of actuating core cooling functions diverse from the plant main control room.*

*In summary, the ABWR design has incorporated defense-in-depth principles through maintaining separation of control and protection functions even though sensors are shared within protection systems. In addition, the shared sensors are designed within a full four division architecture with two-out-of-four voting logic.*

*Diversity principles are incorporated at both the signal and system levels: (1) diverse parameters are monitored to automatically initiate protective actions which are also manually controllable; and, (2) multiple diverse systems are available to both shut down the reactor and to cool its core.*

*Therefore, the ABWR fully meets the intent of NUREG-0493.*

### *Items 7A.5(5) and 7A.6(5)*

*NUREG-0491 has been reviewed and determined to be a precursor to NUREG-0493 for which GE has stated full compliance as detailed above. Therefore, the ABWR design is also consistent with the intent of NUREG-0491.*

### *Items 6(1) and 6(3)*

*IEEE-603 has been reviewed, as has Regulatory Guide 1.153 which endorses IEEE-603.*

*The microprocessor hardware and software which make up the Safety System Logic and Control (SSLC) is designed to make logic decisions which automatically initiate safety actions based on input from instrument monitored parameters for several nuclear safety systems. As shown in Figure 7.1-2 of Section 7.1 and Figure 7A-1, the SSLC is not a nuclear safety system of itself, but is a means by which the nuclear safety systems accomplish their functions. In that sense, the SSLC is a component that integrates the nuclear safety systems.*

*Most positions stated in IEEE-603 (as endorsed by RG 1.153) pertain to the nuclear safety systems, and are similar to those of IEEE-279, which are addressed for each system in the analysis sections of Chapter 7. Safety system design bases are described for all I&C systems in Section 7.1, beginning at Subsection 7.1.2.2. Setpoints and margin may be found in Chapter 16.*

*The safety system criteria in Section 5 of IEEE-603 are not compromised by the introduction of the SSLC. All positions regarding single-failure, completion of protective actions, etc., are designed into the protection systems. All SSLC components associated with the protection systems are Class 1E and are qualified to the same standards as the protection systems.*

*Independence of the four SSLC electrical divisions is retained by using fiber-optic cable for cross-divisional communication such as the two-out-of-four voting logic. Capability for test and calibration is greatly enhanced by the SSLC's self-test subsystem (STS) as described in Subsection 7.1.2.1.6.*

*In summary, the hardware and software functions of the microprocessors used in the SSLC comply with applicable portions of IEEE-603 and Regulatory Guide 1.153 (i.e., quality, qualification, testability, independence). The remaining portions, which apply to the nuclear safety systems, are not compromised by the SSLC design, but are in fact enhanced by self-test.*]*

* See Section 7A.1(1).

## Table 7A-1 List of Equipment Interface with Essential MUX Signals

| Device | Div | Description |
|---|---|---|
| B21-F003A | 1 | AO CHECK VALVE |
| B21-F003B | 2 | AO CHECK VALVE |
| B21-F010A | 1 | SRV/ADS VALVE |
| B21-F010A | 2 | SRV/ADS VALVE |
| B21-F010A | 3 | SRV/ADS VALVE |
| B21-F010B | 3 | SAFETY RELIEF VALVE |
| B21-F010C | 1 | SRV/ADS VALVE |
| B21-F010C | 2 | SRV/ADS VALVE |
| B21-F010D | 1 | SAFETY RELIEF VALVE |
| B21-F010E | 2 | SAFETY RELIEF VALVE |
| B21-F010F | 1 | SRV/ADS VALVE |
| B21-F010F | 2 | SRV/ADS VALVE |
| B21-F010G | 1 | SAFETY RELIEF VALVE |
| B21-F010H | 1 | SRV/ADS VALVE |
| B21-F010H | 2 | SRV/ADS VALVE |
| B21-F010H | 3 | SRV/ADS VALVE |
| B21-F010J | 2 | SAFETY RELIEF VALVE |
| B21-F010K | 1 | SAFETY RELIEF VALVE |
| B21-F010L | 1 | SRV/ADS VALVE |
| B21-F010L | 2 | SRV/ADS VALVE |
| B21-F010L | 3 | SRV/ADS VALVE |
| B21-F010M | 3 | SAFETY RELIEF VALVE |
| B21-F010N | 1 | SRV/ADS VALVE |
| B21-F010N | 2 | SRV/ADS VALVE |
| B21-F010P | 1 | SAFETY RELIEF VALVE |
| B21-F010R | 1 | SRV/ADS VALVE |
| B21-F010R | 2 | SRV/ADS VALVE |
| B21-F010S | 2 | SAFETY RELIEF VALVE |
| B21-F010T | 1 | SRV/ADS VALVE |
| B21-F010T | 2 | SRV/ADS VALVE |
| B21-F010U | 3 | SAFETY RELIEF VALVE |
| B21-F011 | 1 | MO GATE VALVE |
| B21-F012 | 2 | MO GATE VALVE |
| B21-LT001A | 1 | LEVEL TRANSMITTER |
| B21-LT001B | 2 | LEVEL TRANSMITTER |
| B21-LT001C | 3 | LEVEL TRANSMITTER |

## Table 7A-1 List of Equipment Interface with Essential MUX Signals (Continued)

| Device | Div | Description |
|---|---|---|
| B21-LT001D | 4 | LEVEL TRANSMITTER |
| B21-LT003A | 1 | LEVEL TRANSMITTER |
| B21-LT003B | 2 | LEVEL TRANSMITTER |
| B21-LT003C | 3 | LEVEL TRANSMITTER |
| B21-LT003D | 4 | LEVEL TRANSMITTER |
| B21-LT003E | 1 | LEVEL TRANSMITTER |
| B21-LT003F | 2 | LEVEL TRANSMITTER |
| B21-LT003G | 3 | LEVEL TRANSMITTER |
| B21-LT003H | 4 | LEVEL TRANSMITTER |
| B21-LT006A | 1 | LEVEL TRANSMITTER |
| B21-LT006B | 2 | LEVEL TRANSMITTER |
| B21-POSZ902A | 3 | POSITION SWITCH |
| B21-POSZ902B | 3 | POSITION SWITCH |
| B21-POSZ902C | 2 | POSITION SWITCH |
| B21-POSZ902D | 1 | POSITION SWITCH |
| B21-POSZ902E | 2 | POSITION SWITCH |
| B21-POSZ902F | 1 | POSITION SWITCH |
| B21-POSZ902G | 1 | POSITION SWITCH |
| B21-POSZ902H | 3 | POSITION SWITCH |
| B21-POSZ902J | 2 | POSITION SWITCH |
| B21-POSZ902K | 1 | POSITION SWITCH |
| B21-POSZ902L | 3 | POSITION SWITCH |
| B21-POSZ902M | 3 | POSITION SWITCH |
| B21-POSZ902N | 2 | POSITION SWITCH |
| B21-POSZ902P | 1 | POSITION SWITCH |
| B21-POSZ902R | 2 | POSITION SWITCH |
| B21-POSZ902S | 2 | POSITION SWITCH |
| B21-POSZ902T | 1 | POSITION SWITCH |
| B21-POSZ902U | 3 | POSITION SWITCH |
| B21-F010A | 3 | SRV POSITION TRANSMITTER |
| B21-F010B | 3 | SRV POSITION TRANSMITTER |
| B21-F010C | 2 | SRV POSITION TRANSMITTER |
| B21-F010D | 1 | SRV POSITION TRANSMITTER |
| B21-F010E | 2 | SRV POSITION TRANSMITTER |
| B21-F010F | 1 | SRV POSITION TRANSMITTER |
| B21-F010G | 1 | SRV POSITION TRANSMITTER |

## Table 7A-1 List of Equipment Interface with Essential MUX Signals (Continued)

| Device | Div | Description |
|---|---|---|
| B21-F010H | 3 | SRV POSITION TRANSMITTER |
| B21-F010J | 2 | SRV POSITION TRANSMITTER |
| B21-F010K | 1 | SRV POSITION TRANSMITTER |
| B21-F010L | 3 | SRV POSITION TRANSMITTER |
| B21-F010M | 3 | SRV POSITION TRANSMITTER |
| B21-F010N | 2 | SRV POSITION TRANSMITTER |
| B21-F010P | 1 | SRV POSITION TRANSMITTER |
| B21-F010R | 2 | SRV POSITION TRANSMITTER |
| B21-F010S | 2 | SRV POSITION TRANSMITTER |
| B21-F010T | 1 | SRV POSITION TRANSMITTER |
| B21-F010U | 3 | SRV POSITION TRANSMITTER |
| B21-PT007A | 1 | PRESS TRANSMITTER |
| B21-PT007B | 2 | PRESS TRANSMITTER |
| B21-PT007C | 3 | PRESS TRANSMITTER |
| B21-PT007D | 4 | PRESS TRANSMITTER |
| B21-PT025A | 1 | PRESS TRANSMITTER |
| B21-PT025B | 2 | PRESS TRANSMITTER |
| B21-PT025C | 3 | PRESS TRANSMITTER |
| B21-PT025D | 4 | PRESS TRANSMITTER |
| B21-PT028A | 1 | PRESS TRANSMITTER |
| B21-PT028B | 2 | PRESS TRANSMITTER |
| B21-PT028C | 3 | PRESS TRANSMITTER |
| B21-PT028D | 4 | PRESS TRANSMITTER |
| B21-PT301A | 1 | PRESS TRANSMITTER |
| B21-PT301B | 2 | PRESS TRANSMITTER |
| B21-PT301C | 3 | PRESS TRANSMITTER |
| B21-PT301D | 4 | PRESS TRANSMITTER |
| B21-TE019A | 1 | TEMP ELEMENT |
| B21-TE019B | 2 | TEMP ELEMENT |
| B21-TE020A | 1 | TEMP ELEMENT |
| B21-TE020B | 2 | TEMP ELEMENT |
| B21-TE021A | 1 | TEMP ELEMENT |
| B21-TE021B | 2 | TEMP ELEMENT |
| B21-TE022A | 1 | TEMP ELEMENT |
| B21-TE022B | 2 | TEMP ELEMENT |
| B21-TE023A | 1 | TEMP ELEMENT |

## Table 7A-1 List of Equipment Interface with Essential MUX Signals (Continued)

| Device | Div | Description |
|---|---|---|
| B21-TE023B | 2 | TEMP ELEMENT |
| B21-TE024A | 1 | TEMP ELEMENT |
| B21-TE024B | 2 | TEMP ELEMENT |
| C12-D005001 | 1 | FMCRD 34-63 A QUAD |
| C12-D005001 | 2 | FMCRD 34-63 A QUAD |
| C12-D005002 | 1 | FMCRD 54-59 A QUAD |
| C12-D005002 | 2 | FMCRD 54-59 A QUAD |
| C12-D005003 | 1 | FMCRD 38-19 C QUAD |
| C12-D005003 | 2 | FMCRD 38-19 C QUAD |
| C12-D005004 | 1 | FMCRD 50-59 A QUAD |
| C12-D005004 | 2 | FMCRD 50-59 A QUAD |
| C12-D005005 | 1 | FMCRD 38-35 A QUAD |
| C12-D005005 | 2 | FMCRD 38-35 A QUAD |
| C12-D005006 | 1 | FMCRD 54-35 C QUAD |
| C12-D005006 | 2 | FMCRD 54-35 C QUAD |
| C12-D005007 | 1 | FMCRD 34-23 C QUAD |
| C12-D005007 | 2 | FMCRD 34-23 C QUAD |
| C12-D005008 | 1 | FMCRD 50-55 A QUAD |
| C12-D005008 | 2 | FMCRD 50-55 A QUAD |
| C12-D005009 | 1 | FMCRD 62-47 A QUAD |
| C12-D005009 | 2 | FMCRD 62-47 A QUAD |
| C12-D005010 | 1 | FMCRD 38-31 C QUAD |
| C12-D005010 | 2 | FMCRD 38-31 C QUAD |
| C12-D005011 | 1 | FMCRD 58-35 C QUAD |
| C12-D005011 | 2 | FMCRD 58-35 C QUAD |
| C12-D005012 | 1 | FMCRD 58-47 A QUAD |
| C12-D005012 | 2 | FMCRD 58-47 A QUAD |
| C12-D005013 | 1 | FMCRD 42-27 C QUAD |
| C12-D005013 | 2 | FMCRD 42-27 C QUAD |
| C12-D005014 | 1 | FMCRD 54-47 A QUAD |
| C12-D005014 | 2 | FMCRD 54-47 A QUAD |
| C12-D005015 | 1 | FMCRD 46-63 A QUAD |
| C12-D005015 | 2 | FMCRD 46-63 A QUAD |
| C12-D005016 | 1 | FMCRD 50-51 A QUAD |
| C12-D005016 | 2 | FMCRD 50-51 A QUAD |
| C12-D005017 | 1 | FMCRD 46-59 A QUAD |

## Table 7A-1 List of Equipment Interface with Essential MUX Signals (Continued)

| Device | Div | Description |
|---|---|---|
| C12-D005017 | 2 | FMCRD 46-59 A QUAD |
| C12-D005018 | 1 | FMCRD 42-23 C QUAD |
| C12-D005018 | 2 | FMCRD 42-23 C QUAD |
| C12-D005019 | 1 | FMCRD 38-27 C QUAD |
| C12-D005019 | 2 | FMCRD 38-27 C QUAD |
| C12-D005020 | 1 | FMCRD 38-55 A QUAD |
| C12-D005020 | 2 | FMCRD 38-55 A QUAD |
| C12-D005021 | 1 | FMCRD 34-67 A QUAD |
| C12-D005021 | 2 | FMCRD 34-67 A QUAD |
| C12-D005022 | 1 | FMCRD 26-07 B QUAD |
| C12-D005022 | 2 | FMCRD 26-07 B QUAD |
| C12-D005023 | 1 | FMCRD 38-03 C QUAD |
| C12-D005023 | 2 | FMCRD 38-03 C QUAD |
| C12-D005024 | 1 | FMCRD 10-43 D QUAD |
| C12-D005024 | 2 | FMCRD 10-43 D QUAD |
| C12-D005025 | 1 | FMCRD 42-35 A QUAD |
| C12-D005025 | 2 | FMCRD 42-35 A QUAD |
| C12-D005026 | 1 | FMCRD 14-11 B QUAD |
| C12-D005026 | 2 | FMCRD 14-11 B QUAD |
| C12-D005027 | 1 | FMCRD 54-51 A QUAD |
| C12-D005027 | 2 | FMCRD 54-51 A QUAD |
| C12-D005028 | 1 | FMCRD 34-39 D QUAD |
| C12-D005028 | 2 | FMCRD 34-39 D QUAD |
| C12-D005029 | 1 | FMCRD 34-19 C QUAD |
| C12-D005029 | 2 | FMCRD 34-19 C QUAD |
| C12-D005030 | 1 | FMCRD 10-19 B QUAD |
| C12-D005030 | 2 | FMCRD 10-19 B QUAD |
| C12-D005031 | 1 | FMCRD 30-23 B QUAD |
| C12-D005031 | 2 | FMCRD 30-23 B QUAD |
| C12-D005032 | 1 | FMCRD 22-47 D QUAD |
| C12-D005032 | 2 | FMCRD 22-47 D QUAD |
| C12-D005033 | 1 | FMCRD 54-31 C QUAD |
| C12-D005033 | 2 | FMCRD 54-31 C QUAD |
| C12-D005034 | 1 | FMCRD 06-47 D QUAD |
| C12-D005034 | 2 | FMCRD 06-47 D QUAD |
| C12-D005035 | 1 | FMCRD 22-19 B QUAD |

## Table 7A-1 List of Equipment Interface with Essential MUX Signals (Continued)

| Device | Div | Description |
|---|---|---|
| C12-D005035 | 2 | FMCRD 22-19 B QUAD |
| C12-D005036 | 1 | FMCRD 34-43 D QUAD |
| C12-D005036 | 2 | FMCRD 34-43 D QUAD |
| C12-D005037 | 1 | FMCRD 50-31 C QUAD |
| C12-D005037 | 2 | FMCRD 50-31 C QUAD |
| C12-D005038 | 1 | FMCRD 42-19 C QUAD |
| C12-D005038 | 2 | FMCRD 42-19 C QUAD |
| C12-D005039 | 1 | FMCRD 30-19 B QUAD |
| C12-D005039 | 2 | FMCRD 30-19 B QUAD |
| C12-D005040 | 1 | FMCRD 38-67 A QUAD |
| C12-D005040 | 2 | FMCRD 38-67 A QUAD |
| C12-D005041 | 1 | FMCRD 46-47 A QUAD |
| C12-D005041 | 2 | FMCRD 46-47 A QUAD |
| C12-D005042 | 1 | FMCRD 42-59 A QUAD |
| C12-D005042 | 2 | FMCRD 42-59 A QUAD |
| C12-D005043 | 1 | FMCRD 26-39 D QUAD |
| C12-D005043 | 2 | FMCRD 26-39 D QUAD |
| C12-D005044 | 1 | FMCRD 42-11 C QUAD |
| C12-D005044 | 2 | FMCRD 42-11 C QUAD |
| C12-D005045 | 1 | FMCRD 46-15 C QUAD |
| C12-D005045 | 2 | FMCRD 46-15 C QUAD |
| C12-D005046 | 1 | FMCRD 34-31 C QUAD |
| C12-D005046 | 2 | FMCRD 34-31 C QUAD |
| C12-D005047 | 1 | FMCRD 10-15 B QUAD |
| C12-D005047 | 2 | FMCRD 10-15 B QUAD |
| C12-D005048 | 1 | FMCRD 46-35 A QUAD |
| C12-D005048 | 2 | FMCRD 46-35 A QUAD |
| C12-D005049 | 1 | FMCRD 46-19 C QUAD |
| C12-D005049 | 2 | FMCRD 46-19 C QUAD |
| C12-D005050 | 1 | FMCRD 58-27 C QUAD |
| C12-D005050 | 2 | FMCRD 58-27 C QUAD |
| C12-D005051 | 1 | FMCRD 26-15 B QUAD |
| C12-D005051 | 2 | FMCRD 26-15 B QUAD |
| C12-D005052 | 1 | FMCRD 54-19 C QUAD |
| C12-D005052 | 2 | FMCRD 54-19 C QUAD |
| C12-D005053 | 1 | FMCRD 50-23 C QUAD |

## Table 7A-1 List of Equipment Interface with Essential MUX Signals (Continued)

| Device | Div | Description |
|---|---|---|
| C12-D005053 | 2 | FMCRD 50-23 C QUAD |
| C12-D005054 | 1 | FMCRD 66-35 C QUAD |
| C12-D005054 | 2 | FMCRD 66-35 C QUAD |
| C12-D005055 | 1 | FMCRD 06-39 D QUAD |
| C12-D005055 | 2 | FMCRD 06-39 D QUAD |
| C12-D005056 | 1 | FMCRD 66-39 A QUAD |
| C12-D005056 | 2 | FMCRD 66-39 A QUAD |
| C12-D005057 | 1 | FMCRD 06-31 B QUAD |
| C12-D005057 | 2 | FMCRD 06-31 B QUAD |
| C12-D005058 | 1 | FMCRD 58-51 A QUAD |
| C12-D005058 | 2 | FMCRD 58-51 A QUAD |
| C12-D005059 | 1 | FMCRD 58-23 C QUAD |
| C12-D005059 | 2 | FMCRD 58-23 C QUAD |
| C12-D005060 | 1 | FMCRD 34-27 C QUAD |
| C12-D005060 | 2 | FMCRD 34-27 C QUAD |
| C12-D005061 | 1 | FMCRD 22-27 B QUAD |
| C12-D005061 | 2 | FMCRD 22-27 B QUAD |
| C12-D005062 | 1 | FMCRD 50-43 A QUAD |
| C12-D005062 | 2 | FMCRD 50-43 A QUAD |
| C12-D005063 | 1 | FMCRD 38-51 A QUAD |
| C12-D005063 | 2 | FMCRD 38-51 A QUAD |
| C12-D005064 | 1 | FMCRD 58-31 C QUAD |
| C12-D005064 | 2 | FMCRD 58-31 C QUAD |
| C12-D005065 | 1 | FMCRD 14-27 B QUAD |
| C12-D005065 | 2 | FMCRD 14-27 B QUAD |
| C12-D005066 | 1 | FMCRD 50-47 A QUAD |
| C12-D005066 | 2 | FMCRD 50-47 A QUAD |
| C12-D005067 | 1 | FMCRD 38-47 A QUAD |
| C12-D005067 | 2 | FMCRD 38-47 A QUAD |
| C12-D005068 | 1 | FMCRD 46-55 A QUAD |
| C12-D005068 | 2 | FMCRD 46-55 A QUAD |
| C12-D005069 | 1 | FMCRD 26-27 B QUAD |
| C12-D005069 | 2 | FMCRD 26-27 B QUAD |
| C12-D005070 | 1 | FMCRD 58-55 A QUAD |
| C12-D005070 | 2 | FMCRD 58-55 A QUAD |
| C12-D005071 | 1 | FMCRD 58-39 A QUAD |

## Table 7A-1 List of Equipment Interface with Essential MUX Signals (Continued)

| Device | Div | Description |
|---|---|---|
| C12-D005071 | 2 | FMCRD 58-39 A QUAD |
| C12-D005072 | 1 | FMCRD 38-11 C QUAD |
| C12-D005072 | 2 | FMCRD 38-11 C QUAD |
| C12-D005073 | 1 | FMCRD 42-31 C QUAD |
| C12-D005073 | 2 | FMCRD 42-31 C QUAD |
| C12-D005074 | 1 | FMCRD 26-11 B QUAD |
| C12-D005074 | 2 | FMCRD 26-11 B QUAD |
| C12-D005075 | 1 | FMCRD 50-15 C QUAD |
| C12-D005075 | 2 | FMCRD 50-15 C QUAD |
| C12-D005076 | 1 | FMCRD 34-15 B QUAD |
| C12-D005076 | 2 | FMCRD 34-15 B QUAD |
| C12-D005077 | 1 | FMCRD 38-43 A QUAD |
| C12-D005077 | 2 | FMCRD 38-43 A QUAD |
| C12-D005078 | 1 | FMCRD 22-43 D QUAD |
| C12-D005078 | 2 | FMCRD 22-43 D QUAD |
| C12-D005079 | 1 | FMCRD 58-43 A QUAD |
| C12-D005079 | 2 | FMCRD 58-43 A QUAD |
| C12-D005080 | 1 | FMCRD 14-59 D QUAD |
| C12-D005080 | 2 | FMCRD 14-59 D QUAD |
| C12-D005081 | 1 | FMCRD 42-15 C QUAD |
| C12-D005081 | 2 | FMCRD 42-15 C QUAD |
| C12-D005082 | 1 | FMCRD 18-23 B QUAD |
| C12-D005082 | 2 | FMCRD 18-23 B QUAD |
| C12-D005083 | 1 | FMCRD 42-43 A QUAD |
| C12-D005083 | 2 | FMCRD 42-43 A QUAD |
| C12-D005084 | 1 | FMCRD 06-35 D QUAD |
| C12-D005084 | 2 | FMCRD 06-35 D QUAD |
| C12-D005085 | 1 | FMCRD 42-51 A QUAD |
| C12-D005085 | 2 | FMCRD 42-51 A QUAD |
| C12-D005086 | 1 | FMCRD 18-59 D QUAD |
| C12-D005086 | 2 | FMCRD 18-59 D QUAD |
| C12-D005087 | 1 | FMCRD 42-07 C QUAD |
| C12-D005087 | 2 | FMCRD 42-07 C QUAD |
| C12-D005088 | 1 | FMCRD 14-43 D QUAD |
| C12-D005088 | 2 | FMCRD 14-43 D QUAD |
| C12-D005089 | 1 | FMCRD 18-35 D QUAD |

## Table 7A-1 List of Equipment Interface with Essential MUX Signals (Continued)

| Device | Div | Description |
|---|---|---|
| C12-D005089 | 2 | FMCRD 18-35 D QUAD |
| C12-D005090 | 1 | FMCRD 26-31 B QUAD |
| C12-D005090 | 2 | FMCRD 26-31 B QUAD |
| C12-D005091 | 1 | FMCRD 46-51 A QUAD |
| C12-D005091 | 2 | FMCRD 46-51 A QUAD |
| C12-D005092 | 1 | FMCRD 22-11 B QUAD |
| C12-D005092 | 2 | FMCRD 22-11 B QUAD |
| C12-D005093 | 1 | FMCRD 22-55 D QUAD |
| C12-D005093 | 2 | FMCRD 22-55 D QUAD |
| C12-D005094 | 1 | FMCRD 22-59 D QUAD |
| C12-D005094 | 2 | FMCRD 22-59 D QUAD |
| C12-D005095 | 1 | FMCRD 26-63 D QUAD |
| C12-D005095 | 2 | FMCRD 26-63 D QUAD |
| C12-D005096 | 1 | FMCRD 14-23 B QUAD |
| C12-D005096 | 2 | FMCRD 14-23 B QUAD |
| C12-D005097 | 1 | FMCRD 22-35 B QUAD |
| C12-D005097 | 2 | FMCRD 22-35 B QUAD |
| C12-D005098 | 1 | FMCRD 30-27 B QUAD |
| C12-D005098 | 2 | FMCRD 30-27 B QUAD |
| C12-D005099 | 1 | FMCRD 34-11 B QUAD |
| C12-D005099 | 2 | FMCRD 34-11 B QUAD |
| C12-D005100 | 1 | FMCRD 18-47 D QUAD |
| C12-D005100 | 2 | FMCRD 18-47 D QUAD |
| C12-D005101 | 1 | FMCRD 62-23 C QUAD |
| C12-D005101 | 2 | FMCRD 62-23 C QUAD |
| C12-D005102 | 1 | FMCRD 10-51 D QUAD |
| C12-D005102 | 2 | FMCRD 10-51 D QUAD |
| C12-D005103 | 1 | FMCRD 34-51 D QUAD |
| C12-D005103 | 2 | FMCRD 34-51 D QUAD |
| C12-D005104 | 1 | FMCRD 14-47 D QUAD |
| C12-D005104 | 2 | FMCRD 14-47 D QUAD |
| C12-D005105 | 1 | FMCRD 62-27 C QUAD |
| C12-D005105 | 2 | FMCRD 62-27 C QUAD |
| C12-D005106 | 1 | FMCRD 26-55 D QUAD |
| C12-D005106 | 2 | FMCRD 26-55 D QUAD |
| C12-D005107 | 1 | FMCRD 30-03 B QUAD |

## Table 7A-1 List of Equipment Interface with Essential MUX Signals (Continued)

| Device | Div | Description |
|---|---|---|
| C12-D005107 | 2 | FMCRD 30-03 B QUAD |
| C12-D005108 | 1 | FMCRD 10-47 D QUAD |
| C12-D005108 | 2 | FMCRD 10-47 D QUAD |
| C12-D005109 | 1 | FMCRD 10-39 D QUAD |
| C12-D005109 | 2 | FMCRD 10-39 D QUAD |
| C12-D005110 | 1 | FMCRD 26-35 B QUAD |
| C12-D005110 | 2 | FMCRD 26-35 B QUAD |
| C12-D005111 | 1 | FMCRD 22-07 B QUAD |
| C12-D005111 | 2 | FMCRD 22-07 B QUAD |
| C12-D005112 | 1 | FMCRD 46-39 A QUAD |
| C12-D005112 | 2 | FMCRD 46-39 A QUAD |
| C12-D005113 | 1 | FMCRD 38-63 A QUAD |
| C12-D005113 | 2 | FMCRD 38-63 A QUAD |
| C12-D005114 | 1 | FMCRD 34-59 A QUAD |
| C12-D005114 | 2 | FMCRD 34-59 A QUAD |
| C12-D005115 | 1 | FMCRD 30-43 D QUAD |
| C12-D005115 | 2 | FMCRD 30-43 D QUAD |
| C12-D005116 | 1 | FMCRD 62-35 C QUAD |
| C12-D005116 | 2 | FMCRD 62-35 C QUAD |
| C12-D005117 | 1 | FMCRD 22-39 D QUAD |
| C12-D005117 | 2 | FMCRD 22-39 D QUAD |
| C12-D005118 | 1 | FMCRD 42-63 A QUAD |
| C12-D005118 | 2 | FMCRD 42-63 A QUAD |
| C12-D005119 | 1 | FMCRD 46-11 C QUAD |
| C12-D005119 | 2 | FMCRD 46-11 C QUAD |
| C12-D005120 | 1 | FMCRD 46-27 C QUAD |
| C12-D005120 | 2 | FMCRD 46-27 C QUAD |
| C12-D005121 | 1 | FMCRD 30-35 B QUAD |
| C12-D005121 | 2 | FMCRD 30-35 B QUAD |
| C12-D005122 | 1 | FMCRD 38-07 C QUAD |
| C12-D005122 | 2 | FMCRD 38-07 C QUAD |
| C12-D005123 | 1 | FMCRD 18-27 B QUAD |
| C12-D005123 | 2 | FMCRD 18-27 B QUAD |
| C12-D005124 | 1 | FMCRD 42-47 A QUAD |
| C12-D005124 | 2 | FMCRD 42-47 A QUAD |
| C12-D005125 | 1 | FMCRD 34-07 B QUAD |

## Table 7A-1 List of Equipment Interface with Essential MUX Signals (Continued)

| Device | Div | Description |
|---|---|---|
| C12-D005125 | 2 | FMCRD 34-07 B QUAD |
| C12-D005126 | 1 | FMCRD 62-31 C QUAD |
| C12-D005126 | 2 | FMCRD 62-31 C QUAD |
| C12-D005127 | 1 | FMCRD 06-23 B QUAD |
| C12-D005127 | 2 | FMCRD 06-23 B QUAD |
| C12-D005128 | 1 | FMCRD 46-31 C QUAD |
| C12-D005128 | 2 | FMCRD 46-31 C QUAD |
| C12-D005129 | 1 | FMCRD 10-31 B QUAD |
| C12-D005129 | 2 | FMCRD 10-31 B QUAD |
| C12-D005130 | 1 | FMCRD 62-43 A QUAD |
| C12-D005130 | 2 | FMCRD 62-43 A QUAD |
| C12-D005131 | 1 | FMCRD 30-55 D QUAD |
| C12-D005131 | 2 | FMCRD 30-55 D QUAD |
| C12-D005132 | 1 | FMCRD 26-43 D QUAD |
| C12-D005132 | 2 | FMCRD 26-43 D QUAD |
| C12-D005133 | 1 | FMCRD 14-35 D QUAD |
| C12-D005133 | 2 | FMCRD 14-35 D QUAD |
| C12-D005134 | 1 | FMCRD 30-47 D QUAD |
| C12-D005134 | 2 | FMCRD 30-47 D QUAD |
| C12-D005135 | 1 | FMCRD 14-15 B QUAD |
| C12-D005135 | 2 | FMCRD 14-15 B QUAD |
| C12-D005136 | 1 | FMCRD 18-31 B QUAD |
| C12-D005136 | 2 | FMCRD 18-31 B QUAD |
| C12-D005137 | 1 | FMCRD 30-51 D QUAD |
| C12-D005137 | 2 | FMCRD 30-51 D QUAD |
| C12-D005138 | 1 | FMCRD 66-31 C QUAD |
| C12-D005138 | 2 | FMCRD 66-31 C QUAD |
| C12-D005139 | 1 | FMCRD 30-15 B QUAD |
| C12-D005139 | 2 | FMCRD 30-15 B QUAD |
| C12-D005140 | 1 | FMCRD 50-19 C QUAD |
| C12-D005140 | 2 | FMCRD 50-19 C QUAD |
| C12-D005141 | 1 | FMCRD 02-35 D QUAD |
| C12-D005141 | 2 | FMCRD 02-35 D QUAD |
| C12-D005142 | 1 | FMCRD 46-43 A QUAD |
| C12-D005142 | 2 | FMCRD 46-43 A QUAD |
| C12-D005143 | 1 | FMCRD 26-19 B QUAD |

## Table 7A-1 List of Equipment Interface with Essential MUX Signals (Continued)

| Device | Div | Description |
|---|---|---|
| C12-D005143 | 2 | FMCRD 26-19 B QUAD |
| C12-D005144 | 1 | FMCRD 18-15 B QUAD |
| C12-D005144 | 2 | FMCRD 18-15 B QUAD |
| C12-D005145 | 1 | FMCRD 06-43 D QUAD |
| C12-D005145 | 2 | FMCRD 06-43 D QUAD |
| C12-D005146 | 1 | FMCRD 30-59 D QUAD |
| C12-D005146 | 2 | FMCRD 30-59 D QUAD |
| C12-D005147 | 1 | FMCRD 18-43 D QUAD |
| C12-D005147 | 2 | FMCRD 18-43 D QUAD |
| C12-D005148 | 1 | FMCRD 38-59 A QUAD |
| C12-D005148 | 2 | FMCRD 38-59 A QUAD |
| C12-D005149 | 1 | FMCRD 22-15 B QUAD |
| C12-D005149 | 2 | FMCRD 22-15 B QUAD |
| C12-D005150 | 1 | FMCRD 54-27 C QUAD |
| C12-D005150 | 2 | FMCRD 54-27 C QUAD |
| C12-D005151 | 1 | FMCRD 26-51 D QUAD |
| C12-D005151 | 2 | FMCRD 26-51 D QUAD |
| C12-D005152 | 1 | FMCRD 10-35 D QUAD |
| C12-D005152 | 2 | FMCRD 10-35 D QUAD |
| C12-D005153 | 1 | FMCRD 30-07 B QUAD |
| C12-D005153 | 2 | FMCRD 30-07 B QUAD |
| C12-D005154 | 1 | FMCRD 30-31 B QUAD |
| C12-D005154 | 2 | FMCRD 30-31 B QUAD |
| C12-D005155 | 1 | FMCRD 18-51 D QUAD |
| C12-D005155 | 2 | FMCRD 18-51 D QUAD |
| C12-D005156 | 1 | FMCRD 18-39 D QUAD |
| C12-D005156 | 2 | FMCRD 18-39 D QUAD |
| C12-D005157 | 1 | FMCRD 14-55 D QUAD |
| C12-D005157 | 2 | FMCRD 14-55 D QUAD |
| C12-D005158 | 1 | FMCRD 30-39 D QUAD |
| C12-D005158 | 2 | FMCRD 30-39 D QUAD |
| C12-D005159 | 1 | FMCRD 30-11 B QUAD |
| C12-D005159 | 2 | FMCRD 30-11 B QUAD |
| C12-D005160 | 1 | FMCRD 26-23 B QUAD |
| C12-D005160 | 2 | FMCRD 26-23 B QUAD |
| C12-D005161 | 1 | FMCRD 18-55 D QUAD |

## Table 7A-1 List of Equipment Interface with Essential MUX Signals (Continued)

| Device | Div | Description |
|---|---|---|
| C12-D005161 | 2 | FMCRD 18-55 D QUAD |
| C12-D005162 | 1 | FMCRD 18-11 B QUAD |
| C12-D005162 | 2 | FMCRD 18-11 B QUAD |
| C12-D005163 | 1 | FMCRD 14-51 D QUAD |
| C12-D005163 | 2 | FMCRD 14-51 D QUAD |
| C12-D005164 | 1 | FMCRD 18-19 B QUAD |
| C12-D005164 | 2 | FMCRD 18-19 B QUAD |
| C12-D005165 | 1 | FMCRD 10-23 B QUAD |
| C12-D005165 | 2 | FMCRD 10-23 B QUAD |
| C12-D005166 | 1 | FMCRD 02-31 B QUAD |
| C12-D005166 | 2 | FMCRD 02-31 B QUAD |
| C12-D005167 | 1 | FMCRD 34-35 B QUAD |
| C12-D005167 | 2 | FMCRD 34-35 B QUAD |
| C12-D005168 | 1 | FMCRD 54-43 A QUAD |
| C12-D005168 | 2 | FMCRD 54-43 A QUAD |
| C12-D005169 | 1 | FMCRD 06-27 B QUAD |
| C12-D005169 | 2 | FMCRD 06-27 B QUAD |
| C12-D005170 | 1 | FMCRD 54-39 A QUAD |
| C12-D005170 | 2 | FMCRD 54-39 A QUAD |
| C12-D005171 | 1 | FMCRD 10-55 D QUAD |
| C12-D005171 | 2 | FMCRD 10-55 D QUAD |
| C12-D005172 | 1 | FMCRD 38-23 C QUAD |
| C12-D005172 | 2 | FMCRD 38-23 C QUAD |
| C12-D005173 | 1 | FMCRD 22-63 D QUAD |
| C12-D005173 | 2 | FMCRD 22-63 D QUAD |
| C12-D005174 | 1 | FMCRD 42-39 A QUAD |
| C12-D005174 | 2 | FMCRD 42-39 A QUAD |
| C12-D005175 | 1 | FMCRD 34-03 B QUAD |
| C12-D005175 | 2 | FMCRD 34-03 B QUAD |
| C12-D005176 | 1 | FMCRD 10-27 B QUAD |
| C12-D005176 | 2 | FMCRD 10-27 B QUAD |
| C12-D005177 | 1 | FMCRD 30-67 D QUAD |
| C12-D005177 | 2 | FMCRD 30-67 D QUAD |
| C12-D005178 | 1 | FMCRD 46-23 C QUAD |
| C12-D005178 | 2 | FMCRD 46-23 C QUAD |
| C12-D005179 | 1 | FMCRD 02-39 D QUAD |

## Table 7A-1 List of Equipment Interface with Essential MUX Signals (Continued)

| Device | Div | Description |
|---|---|---|
| C12-D005179 | 2 | FMCRD 02-39 D QUAD |
| C12-D005180 | 1 | FMCRD 14-31 B QUAD |
| C12-D005180 | 2 | FMCRD 14-31 B QUAD |
| C12-D005181 | 1 | FMCRD 14-39 D QUAD |
| C12-D005181 | 2 | FMCRD 14-39 D QUAD |
| C12-D005182 | 1 | FMCRD 22-31 B QUAD |
| C12-D005182 | 2 | FMCRD 22-31 B QUAD |
| C12-D005183 | 1 | FMCRD 62-39 A QUAD |
| C12-D005183 | 2 | FMCRD 62-39 A QUAD |
| C12-D005184 | 1 | FMCRD 34-47 D QUAD |
| C12-D005184 | 2 | FMCRD 34-47 D QUAD |
| C12-D005185 | 1 | FMCRD 58-19 C QUAD |
| C12-D005185 | 2 | FMCRD 58-19 C QUAD |
| C12-D005186 | 1 | FMCRD 22-51 D QUAD |
| C12-D005186 | 2 | FMCRD 22-51 D QUAD |
| C12-D005187 | 1 | FMCRD 50-35 C QUAD |
| C12-D005187 | 2 | FMCRD 50-35 C QUAD |
| C12-D005188 | 1 | FMCRD 54-11 C QUAD |
| C12-D005188 | 2 | FMCRD 54-11 C QUAD |
| C12-D005189 | 1 | FMCRD 38-15 C QUAD |
| C12-D005189 | 2 | FMCRD 38-15 C QUAD |
| C12-D005190 | 1 | FMCRD 42-55 A QUAD |
| C12-D005190 | 2 | FMCRD 42-55 A QUAD |
| C12-D005191 | 1 | FMCRD 38-39 A QUAD |
| C12-D005191 | 2 | FMCRD 38-39 A QUAD |
| C12-D005192 | 1 | FMCRD 54-23 C QUAD |
| C12-D005192 | 2 | FMCRD 54-23 C QUAD |
| C12-D005193 | 1 | FMCRD 50-39 A QUAD |
| C12-D005193 | 2 | FMCRD 50-39 A QUAD |
| C12-D005194 | 1 | FMCRD 26-47 D QUAD |
| C12-D005194 | 2 | FMCRD 26-47 D QUAD |
| C12-D005195 | 1 | FMCRD 46-07 C QUAD |
| C12-D005195 | 2 | FMCRD 46-07 C QUAD |
| C12-D005196 | 1 | FMCRD 22-23 B QUAD |
| C12-D005196 | 2 | FMCRD 22-23 B QUAD |
| C12-D005197 | 1 | FMCRD 54-15 C QUAD |

## Table 7A-1 List of Equipment Interface with Essential MUX Signals (Continued)

| Device | Div | Description |
|---|---|---|
| C12-D005197 | 2 | FMCRD 54-15 C QUAD |
| C12-D005198 | 1 | FMCRD 34-55 A QUAD |
| C12-D005198 | 2 | FMCRD 34-55 A QUAD |
| C12-D005199 | 1 | FMCRD 50-11 C QUAD |
| C12-D005199 | 2 | FMCRD 50-11 C QUAD |
| C12-D005200 | 1 | FMCRD 26-59 D QUAD |
| C12-D005200 | 2 | FMCRD 26-59 D QUAD |
| C12-D005201 | 1 | FMCRD 58-15 C QUAD |
| C12-D005201 | 2 | FMCRD 58-15 C QUAD |
| C12-D005202 | 1 | FMCRD 50-27 C QUAD |
| C12-D005202 | 2 | FMCRD 50-27 C QUAD |
| C12-D005203 | 1 | FMCRD 14-19 B QUAD |
| C12-D005203 | 2 | FMCRD 14-19 B QUAD |
| C12-D005204 | 1 | FMCRD 54-55 A QUAD |
| C12-D005204 | 2 | FMCRD 54-55 A QUAD |
| C12-D005205 | 1 | FMCRD 30-63 D QUAD |
| C12-D005205 | 2 | FMCRD 30-63 D QUAD |
| C12-F041 | 1 | SO VALVE |
| C12-F042 | 2 | SO VALVE |
| C12-F043 | 2 | AO VALVE |
| C12-F044 | 2 | AO VALVE |
| C12-F047 | 1 | AO VALVE |
| C12-F048A | 1 | AO VALVE |
| C12-F048B | 2 | AO VALVE |
| C12-F049A | 1 | AO VALVE |
| C12-F049B | 2 | AO VALVE |
| C12-PT011A | 1 | PRESS TRANSMITTER |
| C12-PT011B | 2 | PRESS TRANSMITTER |
| C12-PT011C | 3 | PRESS TRANSMITTER |
| C12-PT011D | 4 | PRESS TRANSMITTER |
| E11-C001A | 1 | RHR PUMP |
| E11-C001B | 2 | RHR PUMP |
| E11-C001C | 3 | RHR PUMP |
| E11-C002A | 1 | SEAL WATER PUMP |
| E11-C002B | 2 | SEAL WATER PUMP |
| E11-C002C | 3 | SEAL WATER PUMP |

## Table 7A-1 List of Equipment Interface with Essential MUX Signals (Continued)

| Device | Div | Description |
|---|---|---|
| E11-F001A | 1 | MO GATE VALVE |
| E11-F001B | 2 | MO GATE VALVE |
| E11-F001C | 3 | MO GATE VALVE |
| E11-F004A | 1 | MO GLOBE VALVE |
| E11-F004B | 2 | MO GLOBE VALVE |
| E11-F004C | 3 | MO GLOBE VALVE |
| E11-F005A | 1 | MO GATE VALVE |
| E11-F005B | 2 | MO GATE VALVE |
| E11-F005C | 3 | MO GATE VALVE |
| E11-F006A | 1 | AO CHECK VALVE |
| E11-F006B | 2 | AO CHECK VALVE |
| E11-F006C | 3 | AO CHECK VALVE |
| E11-F007B | 2 | MAN OPER GATE VALVE |
| E11-F007C | 3 | MAN OPER GATE VALVE |
| E11-F008A | 1 | MO GLOBE VALVE |
| E11-F008B | 2 | MO GLOBE VALVE |
| E11-F008C | 3 | MO GLOBE VALVE |
| E11-F009A | 1 | MAN OPER GATE VALVE |
| E11-F009B | 2 | MAN OPER GATE VALVE |
| E11-F009C | 3 | MAN OPER GATE VALVE |
| E11-F010A | 1 | MO GATE VALVE |
| E11-F010B | 2 | MO GATE VALVE |
| E11-F010C | 3 | MO GATE VALVE |
| E11-F011A | 2 | MO GATE VALVE (RHR ISOL) |
| E11-F011B | 3 | MO GATE VALVE (RHR ISOL) |
| E11-F011C | 1 | MO GATE VALVE (RHR ISOL) |
| E11-F012A | 1 | MO GATE VALVE |
| E11-F012B | 2 | MO GATE VALVE |
| E11-F012C | 3 | MO GATE VALVE |
| E11-F013A | 1 | MO GLOBE VALVE |
| E11-F013B | 2 | MO GLOBE VALVE |
| E11-F013C | 3 | MO GLOBE VALVE |
| E11-F014B | 2 | MO GATE VALVE |
| E11-F014C | 3 | MO GATE VALVE |
| E11-F015B | 2 | MO GATE VALVE |
| E11-F015C | 3 | MO GATE VALVE |

## Table 7A-1 List of Equipment Interface with Essential MUX Signals (Continued)

| Device | Div | Description |
|---|---|---|
| E11-F017B | 2 | MO GLOBE VALVE |
| E11-F017C | 3 | MO GLOBE VALVE |
| E11-F018B | 2 | MO GATE VALVE |
| E11-F018C | 3 | MO GATE VALVE |
| E11-F019B | 2 | MO GATE VALVE |
| E11-F019C | 3 | MO GATE VALVE |
| E11-F021A | 1 | MO GATE VALVE |
| E11-F021B | 2 | MO GATE VALVE |
| E11-F021C | 3 | MO GATE VALVE |
| E11-F029A | 1 | MO GATE VALVE |
| E11-F029B | 2 | MO GATE VALVE |
| E11-F029C | 3 | MO GATE VALVE |
| E11-F030A | 1 | MO GATE VALVE |
| E11-F030B | 2 | MO GATE VALVE |
| E11-F030C | 3 | MO GATE VALVE |
| E11-F031A | 1 | MO GLOBE VALVE |
| E11-F031B | 2 | MO GLOBE VALVE |
| E11-F031C | 3 | MO GLOBE VALVE |
| E11-F036A | 1 | AO GLOBE VALVE |
| E11-F036B | 2 | AO GLOBE VALVE |
| E11-F036C | 3 | AO GLOBE VALVE |
| E11-F043A | 1 | SO VALVE |
| E11-F043B | 2 | SO VALVE |
| E11-F043C | 3 | SO VALVE |
| E11-F044A | 1 | SO VALVE |
| E11-F044B | 2 | SO VALVE |
| E11-F044C | 3 | SO VALVE |
| E11-F045A | 1 | MO GLOBE VALVE |
| E11-F046A | 1 | MO GLOBE VALVE |
| E11-FT008A1 | 1 | FLOW TRANSMITTER |
| E11-FT008A2 | 1 | FLOW TRANSMITTER |
| E11-FT008B1 | 2 | FLOW TRANSMITTER |
| E11-FT008B2 | 2 | FLOW TRANSMITTER |
| E11-FT008C1 | 3 | FLOW TRANSMITTER |
| E11-FT008C2 | 3 | FLOW TRANSMITTER |
| E11-FT012B | 2 | FLOW TRANSMITTER |

## Table 7A-1 List of Equipment Interface with Essential MUX Signals (Continued)

| Device | Div | Description |
|---|---|---|
| E11-FT015B | 2 | FLOW TRANSMITTER |
| E11-FT015C | 3 | FLOW TRANSMITTER |
| E11-POT303A | 1 | POSITION TRANSMITTER |
| E11-POT303B | 2 | POSITION TRANSMITTER |
| E11-POT303C | 3 | POSITION TRANSMITTER |
| E11-PT004A | 1 | PRESS TRANSMITTER |
| E11-PT004B | 2 | PRESS TRANSMITTER |
| E11-PT004C | 3 | PRESS TRANSMITTER |
| E11-PT004E | 1 | PRESS TRANSMITTER |
| E11-PT004F | 2 | PRESS TRANSMITTER |
| E11-PT004G | 3 | PRESS TRANSMITTER |
| E11-PT005A | 1 | PRESS TRANSMITTER |
| E11-PT005B | 2 | PRESS TRANSMITTER |
| E11-PT005C | 3 | PRESS TRANSMITTER |
| E11-PT009A | 1 | PRESS TRANSMITTER |
| E11-PT009B | 2 | PRESS TRANSMITTER |
| E11-PT009C | 3 | PRESS TRANSMITTER |
| E22-C001B | 2 | PUMP |
| E22-C001C | 3 | PUMP |
| E22-F001B | 2 | MO GATE VALVE |
| E22-F001C | 3 | MO GATE VALVE |
| E22-F003B | 2 | MO GATE VALVE |
| E22-F003C | 3 | MO GATE VALVE |
| E22-F004B | 2 | AIR OP CHECK VALVE |
| E22-F004C | 3 | AIR OP CHECK VALVE |
| E22-F005B | 2 | MAN OPER GATE VALVE |
| E22-F005C | 3 | MAN OPER GATE VALVE |
| E22-F006B | 2 | MO GATE VALVE |
| E22-F006C | 3 | MO GATE VALVE |
| E22-F008B | 2 | MO GLOBE VALVE |
| E22-F008C | 3 | MO GLOBE VALVE |
| E22-F009B | 2 | MO GLOBE VALVE |
| E22-F009C | 3 | MO GLOBE VALVE |
| E22-F010B | 2 | MO GATE VALVE |
| E22-F010C | 3 | MO GATE VALVE |
| E22-F019B | 2 | EQUALIZING VALVE |

## Table 7A-1 List of Equipment Interface with Essential MUX Signals (Continued)

| Device | Div | Description |
|---|---|---|
| E22-F019C | 3 | EQUALIZING VALVE |
| E22-FT008B1 | 2 | FLOW TRANSMITTER |
| E22-FT008B2 | 2 | FLOW TRANSMITTER |
| E22-FT008C1 | 3 | FLOW TRANSMITTER |
| E22-FT008C2 | 3 | FLOW TRANSMITTER |
| E22-PT003B | 2 | PRESSURE TRANSMITTER |
| E22-PT003C | 3 | PRESSURE TRANSMITTER |
| E22-PT006B | 2 | PRESSURE TRANSMITTER |
| E22-PT006C | 3 | PRESSURE TRANSMITTER |
| E22-PT006F | 2 | PRESSURE TRANSMITTER |
| E22-PT006G | 3 | PRESSURE TRANSMITTER |
| E22-PT007B | 2 | PRESSURE TRANSMITTER |
| E22-PT007C | 3 | PRESSURE TRANSMITTER |
| E31-DPT006A | 1 | DIFF PRESS TRANSMITTER |
| E31-DPT006B | 2 | DIFF PRESS TRANSMITTER |
| E31-DPT006C | 3 | DIFF PRESS TRANSMITTER |
| E31-DPT006D | 4 | DIFF PRESS TRANSMITTER |
| E31-DPT013A | 1 | DIFF PRESS TRANSMITTER |
| E31-DPT013B | 2 | DIFF PRESS TRANSMITTER |
| E31-DPT013C | 3 | DIFF PRESS TRANSMITTER |
| E31-DPT013D | 4 | DIFF PRESS TRANSMITTER |
| E31-DPT014A | 1 | DIFF PRESS TRANSMITTER |
| E31-DPT014B | 2 | DIFF PRESS TRANSMITTER |
| E31-DPT014C | 3 | DIFF PRESS TRANSMITTER |
| E31-DPT014D | 4 | DIFF PRESS TRANSMITTER |
| E31-DPT015A | 1 | DIFF PRESS TRANSMITTER |
| E31-DPT015B | 2 | DIFF PRESS TRANSMITTER |
| E31-DPT015C | 3 | DIFF PRESS TRANSMITTER |
| E31-DPT015D | 4 | DIFF PRESS TRANSMITTER |
| E31-DPT016A | 1 | DIFF PRESS TRANS |
| E31-DPT016B | 2 | DIFF PRESS TRANS |
| E31-DPT016C | 3 | DIFF PRESS TRANS |
| E31-DPT016D | 4 | DIFF PRESS TRANS |
| E31-DPT016E | 1 | DIFF PRESS TRANS |
| E31-DPT016F | 2 | DIFF PRESS TRANS |
| E31-DPT016G | 3 | DIFF PRESS TRANS |

## Table 7A-1 List of Equipment Interface with Essential MUX Signals (Continued)

| Device | Div | Description |
|---|---|---|
| E31-DPT016H | 4 | DIFF PRESS TRANS |
| E31-DPT016J | 1 | DIFF PRESS TRANS |
| E31-DPT016K | 2 | DIFF PRESS TRANS |
| E31-DPT016L | 3 | DIFF PRESS TRANS |
| E31-DPT016M | 4 | DIFF PRESS TRANS |
| E31-DPT016N | 1 | DIFF PRESS TRANS |
| E31-DPT016P | 2 | DIFF PRESS TRANS |
| E31-DPT016R | 3 | DIFF PRESS TRANS |
| E31-DPT016S | 4 | DIFF PRESS TRANS |
| E31-F002 | 1 | A O SOLENOID VALVE |
| E31-F003 | 2 | A O SOLENOID VALVE |
| E31-F004 | 2 | A O SOLENOID VALVE |
| E31-F005 | 1 | A O SOLENOID VALVE |
| E31-PT007A | 1 | PRESS TRANSMITTER |
| E31-PT007D | 4 | PRESS TRANSMITTER |
| E31-TE005A | 1 | TEMP ELEMENT |
| E31-TE005B | 2 | TEMP ELEMENT |
| E31-TE005C | 3 | TEMP ELEMENT |
| E31-TE005D | 4 | TEMP ELEMENT |
| E31-TE008A | 1 | TEMP ELEMENT |
| E31-TE008B | 2 | TEMP ELEMENT |
| E31-TE008C | 3 | TEMP ELEMENT |
| E31-TE008D | 4 | TEMP ELEMENT |
| E31-TE008E | 1 | TEMP ELEMENT |
| E31-TE008F | 2 | TEMP ELEMENT |
| E31-TE008G | 3 | TEMP ELEMENT |
| E31-TE008H | 4 | TEMP ELEMENT |
| E31-TE008J | 1 | TEMP ELEMENT |
| E31-TE008K | 2 | TEMP ELEMENT |
| E31-TE008L | 3 | TEMP ELEMENT |
| E31-TE008M | 4 | TEMP ELEMENT |
| E31-TE009A | 1 | TEMP ELEMENT |
| E31-TE009B | 2 | TEMP ELEMENT |
| E31-TE009C | 3 | TEMP ELEMENT |
| E31-TE009D | 4 | TEMP ELEMENT |
| E31-TE009E | 1 | TEMP ELEMENT |

## Table 7A-1 List of Equipment Interface with Essential MUX Signals (Continued)

| Device | Div | Description |
|---|---|---|
| E31-TE009F | 2 | TEMP ELEMENT |
| E31-TE009G | 3 | TEMP ELEMENT |
| E31-TE009H | 4 | TEMP ELEMENT |
| E31-TE009J | 1 | TEMP ELEMENT |
| E31-TE009K | 2 | TEMP ELEMENT |
| E31-TE009L | 3 | TEMP ELEMENT |
| E31-TE009M | 4 | TEMP ELEMENT |
| E31-TE010A | 1 | TEMP ELEMENT |
| E31-TE010B | 2 | TEMP ELEMENT |
| E31-TE010C | 3 | TEMP ELEMENT |
| E31-TE010D | 4 | TEMP ELEMENT |
| E31-TE011A | 1 | TEMP ELEMENT |
| E31-TE011B | 2 | TEMP ELEMENT |
| E31-TE011C | 3 | TEMP ELEMENT |
| E31-TE011D | 4 | TEMP ELEMENT |
| E31-TE012A | 1 | TEMP ELEMENT |
| E31-TE012B | 2 | TEMP ELEMENT |
| E31-TE012C | 3 | TEMP ELEMENT |
| E31-TE012D | 4 | TEMP ELEMENT |
| E31-TE018A | 1 | TEMP ELEMENT |
| E31-TE019A | 1 | TEMP ELEMENT |
| E31-TE020A | 1 | TEMP ELEMENT |
| E31-TE020B | 2 | TEMP ELEMENT |
| E31-TE020C | 3 | TEMP ELEMENT |
| E31-TE020D | 4 | TEMP ELEMENT |
| E31-TE021A | 1 | MSL TEMP SENSORS |
| E31-TE021B | 2 | MSL TEMP SENSORS |
| E31-TE021C | 3 | MSL TEMP SENSORS |
| E31-TE021D | 4 | MSL TEMP SENSORS |
| E31-TE022A | 1 | TEMP ELEMENT |
| E31-TE022B | 2 | TEMP ELEMENT |
| E31-TE022C | 3 | TEMP ELEMENT |
| E31-TE022D | 4 | TEMP ELEMENT |
| E31-TE023A | 1 | TEMP ELEMENT |
| E31-TE023B | 2 | TEMP ELEMENT |
| E31-TE023C | 3 | TEMP ELEMENT |

## Table 7A-1 List of Equipment Interface with Essential MUX Signals (Continued)

| Device | Div | Description |
|---|---|---|
| E31-TE023D | 4 | TEMP ELEMENT |
| E31-TE024A | 1 | TEMP ELEMENT |
| E31-TE024B | 2 | TEMP ELEMENT |
| E31-TE024C | 3 | TEMP ELEMENT |
| E31-TE024D | 4 | TEMP ELEMENT |
| E31-TE025A | 1 | TEMP ELEMENT |
| E31-TE025B | 2 | TEMP ELEMENT |
| E31-TE025C | 3 | TEMP ELEMENT |
| E31-TE025D | 4 | TEMP ELEMENT |
| E31-TE026A | 1 | TEMP ELEMENT |
| E31-TE026B | 2 | TEMP ELEMENT |
| E31-TE026C | 3 | TEMP ELEMENT |
| E31-TE026D | 4 | TEMP ELEMENT |
| E31-TE027A | 1 | TEMP ELEMENT |
| E31-TE027B | 2 | TEMP ELEMENT |
| E31-TE027C | 3 | TEMP ELEMENT |
| E31-TE027D | 4 | TEMP ELEMENT |
| E31-TE028A | 1 | TEMP ELEMENT |
| E31-TE028B | 2 | TEMP ELEMENT |
| E31-TE028C | 3 | TEMP ELEMENT |
| E31-TE028D | 4 | TEMP ELEMENT |
| E31-TE029A | 1 | TEMP ELEMENT |
| E31-TE029B | 2 | TEMP ELEMENT |
| E31-TE029C | 3 | TEMP ELEMENT |
| E31-TE029D | 4 | TEMP ELEMENT |
| E31-TE031A | 1 | TEMP ELEMENT |
| E31-TE031E | 1 | TEMP ELEMENT |
| E31-TE031J | 1 | TEMP ELEMENT |
| E31-TE032A | 1 | TEMP ELEMENT |
| E31-TE032E | 1 | TEMP ELEMENT |
| E31-TE032J | 1 | TEMP ELEMENT |
| E31-TE033A | 1 | TEMP ELEMENT |
| E31-TE033E | 1 | TEMP ELEMENT |
| E31-TE033J | 1 | TEMP ELEMENT |
| E31-TE034A | 1 | TEMP ELEMENT |
| E31-TE034E | 1 | TEMP ELEMENT |

## Table 7A-1 List of Equipment Interface with Essential MUX Signals (Continued)

| Device | Div | Description |
|---|---|---|
| E31-TE034J | 1 | TEMP ELEMENT |
| E51-C002 | 1 | TURBINE |
| E51-C901 | 1 | VACUUM PUMP |
| E51-C902 | 1 | CONDENSATE PUMP |
| E51-F001 | 1 | MO GATE VALVE |
| E51-F004 | 1 | MO GATE VALVE |
| E51-F005 | 1 | A0 CHECK VALVE |
| E51-F006 | 1 | MO GATE VALVE |
| E51-F008 | 1 | MO GLOBE VALVE |
| E51-F009 | 1 | MO GLOBE VALVE |
| E51-F011 | 1 | MO GLOBE VALVE |
| E51-F012 | 1 | MO GLOBE VALVE |
| E51-F026 | 1 | AO GLOBE VALVE |
| E51-F031 | 1 | SO DIAPHRAM VALVE |
| E51-F032 | 1 | SO DIAPHRAM VALVE |
| E51-F035 | 1 | MO GATE VALVE |
| E51-F036 | 2 | MO GATE VALVE |
| E51-F037 | 1 | MO GLOBE VALVE |
| E51-F039 | 1 | MO GATE VALVE |
| E51-F040 | 1 | AO GLOBE VALVE |
| E51-F041 | 1 | AO GLOBE VALVE |
| E51-F045 | 1 | MO GLOBE VALVE |
| E51-F047 | 1 | MO GATE VALVE |
| E51-F048 | 1 | MO GLOBE VALVE |
| E51-F058 | 1 | AO GLOBE VALVE |
| E51-FT007-1 | 1 | FLOW TRANSMITTER |
| E51-FT007-2 | 1 | FLOW TRANSMITTER |
| E51-LS011 | 1 | LEVEL SWITCH |
| E51-POT901 | 1 | POSITION TRANSMITTER |
| E51-POT902 | 1 | POSITION TRANSMITTER |
| E51-PT001 | 1 | PRESS TRANSMITTER |
| E51-PT002 | 1 | PRESS TRANSMITTER |
| E51-PT005 | 1 | PRESS TRANSMITTER |
| E51-PT008 | 1 | PRESS TRANSMITTER |
| E51-PT009 | 1 | PRESS TRANSMITTER |
| E51-PT013A | 1 | PRESS TRANSMITTER |

## Table 7A-1 List of Equipment Interface with Essential MUX Signals (Continued)

| Device | Div | Description |
|---|---|---|
| E51-PT013E | 1 | PRESS TRANSMITTER |
| E51-PT014A | 1 | PRESS TRANSMITTER |
| E51-PT014B | 2 | PRESS TRANSMITTER |
| E51-PT014E | 1 | PRESS TRANSMITTER |
| E51-PT014F | 2 | PRESS TRANSMITTER |
| E51-SE997 | 1 | SPEED ELEMENT |
| G31-F002 | 2 | MO GATE VALVE |
| G31-F003 | 1 | MO GATE VALVE |
| G31-F015 | 1 | MO GLOBE VALVE |
| G31-F017 | 1 | MO GATE VALVE |
| G51-F001 | 2 | MO GATE VALVE |
| G51-F002 | 1 | MO GATE VALVE |
| G51-F007 | 2 | MO GATE VALVE |
| K11-C001A | 1 | LCW PUMP - DRYWELL SUMP |
| K11-C001B | 2 | LCW PUMP - DRYWELL SUMP |
| K11-C101A | 1 | HCW PUMP - DRYWELL SUMP |
| K11-C101B | 2 | HCW PUMP - DRYWELL SUMP |
| K11-C102A | 1 | HCW PUMP FOR SUMP (A) |
| K11-C102B | 2 | HCW PUMP FOR SUMP (B) |
| K11-C102C | 3 | HCW PUMP FOR SUMP (C) |
| K11-C102D | 1 | HCW PUMP FOR SUMP (D) |
| K11-C102E | 2 | HCW PUMP FOR SUMP (E) |
| K11-C102F | 3 | HCW PUMP FOR SUMP (A) |
| K11-C102G | 1 | HCW PUMP FOR SUMP (B) |
| K11-C102H | 2 | HCW PUMP FOR SUMP (C) |
| K11-C102I | 3 | HCW PUMP FOR SUMP (D) |
| K11-C102J | 1 | HCW PUMP FOR SUMP (E) |
| P13-LT001A | 1 | COND STORAGE POOL LEVEL |
| P13-LT001B | 2 | COND STORAGE POOL LEVEL |
| P13-LT001C | 3 | COND STORAGE POOL LEVEL |
| P13-LT001D | 4 | COND STORAGE POOL LEVEL |
| P21-C001A | 1 | PUMP |
| P21-C001B | 2 | PUMP |
| P21-C001C | 3 | PUMP |
| P21-C001E | 2 | PUMP |
| P21-C001F | 3 | PUMP |

## Table 7A-1 List of Equipment Interface with Essential MUX Signals (Continued)

| Device | Div | Description |
|---|---|---|
| P21-C001D | 1 | PUMP |
| P21-DPS033A | 1 | DIFF PRESS SWITCH |
| P21-DPS033B | 2 | DIFF PRESS SWITCH |
| P21-DPS033C | 3 | DIFF PRESS SWITCH |
| P21-DPS034A | 1 | DIFF PRESS SWITCH |
| P21-DPS034B | 2 | DIFF PRESS SWITCH |
| P21-DPS034C | 3 | DIFF PRESS SWITCH |
| P21-E/P605A | 1 | E/P CONVERTER |
| P21-E/P605B | 2 | E/P CONVERTER |
| P21-E/P605C | 3 | E/P CONVERTER |
| P21-F004A | 1 | MO GATE VALVE |
| P21-F004B | 2 | MO GATE VALVE |
| P21-F004C | 3 | MO GATE VALVE |
| P21-F004D | 1 | MO GATE VALVE |
| P21-F004E | 2 | MO GATE VALVE |
| P21-F004F | 3 | MO GATE VALVE |
| P21-F004G | 1 | MO GATE VALVE |
| P21-F004H | 2 | MO GATE VALVE |
| P21-F004J | 3 | MO GATE VALVE |
| P21-F013A | 1 | MO GLOBE VALVE |
| P21-F013B | 2 | MO GLOBE VALVE |
| P21-F013C | 3 | MO GLOBE VALVE |
| P21-F018A | 1 | MO GLOBE VALVE |
| P21-F018B | 2 | MO GLOBE VALVE |
| P21-F018C | 3 | MO GLOBE VALVE |
| P21-F019A | 1 | AO GLOBE VALVE |
| P21-F019B | 2 | AO GLOBE VALVE |
| P21-F019C | 3 | AO GLOBE VALVE |
| P21-F025A | 1 | MO GLOBE VALVE |
| P21-F025B | 2 | MO GLOBE VALVE |
| P21-F025C | 3 | MO GLOBE VALVE |
| P21-F025E | 2 | MO GLOBE VALVE |
| P21-F025F | 3 | MO GLOBE VALVE |
| P21-F055A | 1 | MO GATE VALVE |
| P21-F055B | 2 | MO GATE VALVE |
| P21-F055C | 3 | MO GATE VALVE |

## Table 7A-1 List of Equipment Interface with Essential MUX Signals (Continued)

| Device | Div | Description |
|---|---|---|
| P21-F055D | 1 | MO GATE VALVE |
| P21-F055E | 2 | MO GATE VALVE |
| P21-F055F | 3 | MO GATE VALVE |
| P21-F072A | 1 | AO VALVE |
| P21-F072B | 2 | AO VALVE |
| P21-F072C | 3 | AO VALVE |
| P21-F072D | 1 | AO VALVE |
| P21-F072E | 2 | AO VALVE |
| P21-F072F | 3 | AO VALVE |
| P21-F074A | 1 | MO GATE VALVE |
| P21-F074B | 2 | MO GATE VALVE |
| P21-F074C | 3 | MO GATE VALVE |
| P21-F075A | 1 | MO GATE VALVE |
| P21-F075B | 1 | MO GATE VALVE |
| P21-F080A | 2 | MO GATE VALVE |
| P21-F080B | 2 | MO GATE VALVE |
| P21-F081A | 1 | MO GATE VALVE |
| P21-F081B | 1 | MO GATE VALVE |
| P21-F082A | 1 | MO GATE VALVE |
| P21-F082B | 2 | MO GATE VALVE |
| P21-F082C | 3 | MO GATE VALVE |
| P21-F084A | 1 | MAN OPER GATE VALVE |
| P21-F084B | 2 | MAN OPER GATE VALVE |
| P21-F084C | 3 | MAN OPER GATE VALVE |
| P21-F195A | 1 | MO GATE VALVE |
| P21-F195B | 2 | MO GATE VALVE |
| P21-F196A | 1 | MO GATE VALVE |
| P21-F196B | 2 | MO GATE VALVE |
| P21-FT006A | 1 | FLOW TRANSMITTER |
| P21-FT006B | 2 | FLOW TRANSMITTER |
| P21-FT006C | 3 | FLOW TRANSMITTER |
| P21-FT008A | 1 | FLOW TRANSMITTER |
| P21-FT008B | 2 | FLOW TRANSMITTER |
| P21-FT008C | 3 | FLOW TRANSMITTER |
| P21-FT042A | 1 | FLOW TRANSMITTER |
| P21-FT042B | 2 | FLOW TRANSMITTER |

## Table 7A-1 List of Equipment Interface with Essential MUX Signals (Continued)

| Device | Div | Description |
|---|---|---|
| P21-FT042C | 3 | FLOW TRANSMITTER |
| P21-LS015A | 1 | LEVEL SWITCH |
| P21-LS015B | 2 | LEVEL SWITCH |
| P21-LS015C | 3 | LEVEL SWITCH |
| P21-LT013A | 1 | LEVEL TRANSMITTER |
| P21-LT013B | 2 | LEVEL TRANSMITTER |
| P21-LT013C | 3 | LEVEL TRANSMITTER |
| P21-LT014A | 1 | LEVEL TRANSMITTER |
| P21-LT014B | 2 | LEVEL TRANSMITTER |
| P21-LT014C | 3 | LEVEL TRANSMITTER |
| P21-LT014D | 1 | LEVEL TRANSMITTER |
| P21-LT014E | 2 | LEVEL TRANSMITTER |
| P21-LT014F | 3 | LEVEL TRANSMITTER |
| P21-LT014G | 1 | LEVEL TRANSMITTER |
| P21-LT014H | 2 | LEVEL TRANSMITTER |
| P21-LT014J | 3 | LEVEL TRANSMITTER |
| P21-PT004A | 1 | PRESS TRANSMITTER |
| P21-PT004B | 2 | PRESS TRANSMITTER |
| P21-PT004C | 3 | PRESS TRANSMITTER |
| P21-TE005A | 1 | TEMP ELEMENT |
| P21-TE005B | 2 | TEMP ELEMENT |
| P21-TE005C | 3 | TEMP ELEMENT |
| P21-TE009A | 1 | TEMP ELEMENT |
| P21-TE009B | 2 | TEMP ELEMENT |
| P21-TE009C | 3 | TEMP ELEMENT |
| P24-F053 | 1 | MO GATE VALVE |
| P24-F141 | 2 | MO GATE VALVE |
| P24-F142 | 1 | MO GATE VALVE |
| P25 F016A | 1 | TEMP CONTROL VALVE |
| P25-C001A | 1 | HECW PUMP |
| P25-C001B | 2 | HECW PUMP |
| P25-C001C | 3 | HECW PUMP |
| P25-C001E | 2 | HECW PUMP |
| P25-C001F | 3 | HECW PUMP |
| P25-D001A | 1 | REFRIGERATOR |
| P25-D001B | 2 | REFRIGERATOR |

## Table 7A-1 List of Equipment Interface with Essential MUX Signals (Continued)

| Device | Div | Description |
|---|---|---|
| P25-D001C | 3 | REFRIGERATOR |
| P25-D001E | 2 | REFRIGERATOR |
| P25-D001F | 3 | REFRIGERATOR |
| P25-DPT007A | 1 | DIFF PRESS TRANSMITTER |
| P25-DPT007B | 2 | DIFF PRESS TRANSMITTER |
| P25-DPT007C | 3 | DIFF PRESS TRANSMITTER |
| P25-F005B | 2 | TEMP CONTROL VALVE |
| P25-F005C | 3 | TEMP CONTROL VALVE |
| P25-F012A | 1 | PRESSURE CONTROL VALVE |
| P25-F012B | 2 | PRESSURE CONTROL VALVE |
| P25-F012C | 3 | PRESSURE CONTROL VALVE |
| P25-F016B | 2 | TEMP CONTROL VALVE |
| P25-F016C | 3 | TEMP CONTROL VALVE |
| P25-F022A | 1 | TEMP CONTROL VALVE |
| P25-F022B | 2 | TEMP CONTROL VALVE |
| P25-F022C | 3 | TEMP CONTROL VALVE |
| P25-FIS003A | 1 | FLOW IND SWITCH |
| P25-FIS003B | 2 | FLOW IND SWITCH |
| P25-FIS003C | 3 | FLOW IND SWITCH |
| P25-FIS003E | 2 | FLOW IND SWITCH |
| P25-FIS003F | 3 | FLOW IND SWITCH |
| P25-TE005A | 1 | TEMP ELEMENT |
| P25-TE005B | 2 | TEMP ELEMENT |
| P25-TE005C | 3 | TEMP ELEMENT |
| P41-C001A | 1 | RSW PUMP |
| P41-C001B | 2 | RSW PUMP |
| P41-C001C | 3 | RSW PUMP |
| P41-C001D | 1 | RSW PUMP |
| P41-C001E | 2 | RSW PUMP |
| P41-C001F | 3 | RSW PUMP |
| P41-DPI004A | 1 | DIFF PRESS INDICATOR |
| P41-DPI004B | 2 | DIFF PRESS INDICATOR |
| P41-DPI004C | 3 | DIFF PRESS INDICATOR |
| P41-DPI004D | 1 | DIFF PRESS INDICATOR |
| P41-DPI004E | 2 | DIFF PRESS INDICATOR |
| P41-DPI004F | 3 | DIFF PRESS INDICATOR |

## Table 7A-1 List of Equipment Interface with Essential MUX Signals (Continued)

| Device | Div | Description |
|---|---|---|
| P41-DPS004A | 1 | DIFF PRESS SWITCH |
| P41-DPS004B | 2 | DIFF PRESS SWITCH |
| P41-DPS004C | 3 | DIFF PRESS SWITCH |
| P41-DPS004D | 1 | DIFF PRESS SWITCH |
| P41-DPS004E | 2 | DIFF PRESS SWITCH |
| P41-DPS004F | 3 | DIFF PRESS SWITCH |
| P41-DPT004A | 1 | DIFF PRESS TRANS |
| P41-DPT004B | 2 | DIFF PRESS TRANS |
| P41-DPT004C | 3 | DIFF PRESS TRANS |
| P41-DPT004D | 1 | DIFF PRESS TRANS |
| P41-DPT004E | 2 | DIFF PRESS TRANS |
| P41-DPT004F | 3 | DIFF PRESS TRANS |
| P41-F003A | 1 | MO BUTTERFLY VLV |
| P41-F003B | 2 | MO BUTTERFLY VLV |
| P41-F003C | 3 | MO BUTTERFLY VLV |
| P41-F003D | 1 | MO BUTTERFLY VLV |
| P41-F003E | 2 | MO BUTTERFLY VLV |
| P41-F003F | 3 | MO BUTTERFLY VLV |
| P41-F004A | 1 | MO BUTTERFLY VLV |
| P41-F004B | 2 | MO BUTTERFLY VLV |
| P41-F004C | 3 | MO BUTTERFLY VLV |
| P41-F004D | 1 | MO BUTTERFLY VLV |
| P41-F004E | 2 | MO BUTTERFLY VLV |
| P41-F004F | 3 | MO BUTTERFLY VLV |
| P41-F005A | 1 | MO BUTTERFLY VLV |
| P41-F005B | 2 | MO BUTTERFLY VLV |
| P41-F005C | 3 | MO BUTTERFLY VLV |
| P41-F005D | 1 | MO BUTTERFLY VLV |
| P41-F005E | 2 | MO BUTTERFLY VLV |
| P41-F005F | 3 | MO BUTTERFLY VLV |
| P41-F005G | 1 | MO BUTTERFLY VLV |
| P41-F005H | 2 | MO BUTTERFLY VLV |
| P41-F005J | 3 | MO BUTTERFLY VLV |
| P41-F006A | 1 | MO BUTTERFLY VLV |
| P41-F006B | 2 | MO BUTTERFLY VLV |
| P41-F006C | 3 | MO BUTTERFLY VLV |

## Table 7A-1 List of Equipment Interface with Essential MUX Signals (Continued)

| Device | Div | Description |
|---|---|---|
| P41-F006D | 1 | MO BUTTERFLY VLV |
| P41-F006E | 2 | MO BUTTERFLY VLV |
| P41-F006F | 3 | MO BUTTERFLY VLV |
| P41-F009A | 1 | AO GLOBE VALVE |
| P41-F009B | 2 | AO GLOBE VALVE |
| P41-F009C | 3 | AO GLOBE VALVE |
| P41-F009D | 1 | AO GLOBE VALVE |
| P41-F009E | 2 | AO GLOBE VALVE |
| P41-F009F | 3 | AO GLOBE VALVE |
| P41-F009G | 1 | AO GLOBE VALVE |
| P41-F009H | 2 | AO GLOBE VALVE |
| P41-F009J | 3 | AO GLOBE VALVE |
| P41-F011A | 1 | AO GLOBE VALVE |
| P41-F011B | 2 | AO GLOBE VALVE |
| P41-F011C | 3 | AO GLOBE VALVE |
| P41-F011D | 1 | AO GLOBE VALVE |
| P41-F011E | 2 | AO GLOBE VALVE |
| P41-F011F | 3 | AO GLOBE VALVE |
| P41-F011G | 1 | MO BUTTERFLY VLV |
| P41-F011H | 2 | MO BUTTERFLY VLV |
| P41-F011J | 3 | MO BUTTERFLY VLV |
| P41-F013A | 1 | MO BUTTERFLY VLV |
| P41-F013B | 2 | MO BUTTERFLY VLV |
| P41-F013C | 3 | MO BUTTERFLY VLV |
| P41-F013D | 1 | MO BUTTERFLY VLV |
| P41-F013E | 2 | MO BUTTERFLY VLV |
| P41-F013F | 3 | MO BUTTERFLY VLV |
| P41-F014A | 1 | MO BUTTERFLY VLV |
| P41-F014B | 2 | MO BUTTERFLY VLV |
| P41-F014C | 3 | MO BUTTERFLY VLV |
| P41-F015A | 1 | MO BUTTERFLY VLV |
| P41-F015B | 2 | MO BUTTERFLY VLV |
| P41-F015C | 3 | MO BUTTERFLY VLV |
| P41-PT003A | 1 | PRESS TRANSMITTER |
| P41-PT003B | 2 | PRESS TRANSMITTER |
| P41-PT003C | 3 | PRESS TRANSMITTER |

## Table 7A-1 List of Equipment Interface with Essential MUX Signals (Continued)

| Device | Div | Description |
|---|---|---|
| P51-F276 | 1 | MO GLOBE VALVE |
| P54-F003A | 1 | MO GLOBE VALVE |
| P54-F003B | 2 | MO GLOBE VALVE |
| P54-F007A | 1 | MO GLOBE VALVE |
| P54-F007B | 2 | MO GLOBE VALVE |
| P54-F012A | 1 | MO GLOBE VALVE |
| P54-F012B | 2 | MO GLOBE VALVE |
| P54-F200 | 1 | MO GLOBE VALVE |
| P54-PIS001A | 1 | PRESS IND SWITCH |
| P54-PIS001B | 2 | PRESS IND SWITCH |
| P54-PT002A | 1 | PRESS TRANSMITTER |
| P54-PT002B | 2 | PRESS TRANSMITTER |
| P54-PT005 | 1 | PRESS TRANSMITTER |
| R24 MCC C10 | 1 | MOTOR CONTROL CENTER |
| R24 MCC C11 | 1 | MOTOR CONTROL CENTER |
| R24 MCC C12 | 1 | MOTOR CONTROL CENTER |
| R24 MCC C13 | 1 | MOTOR CONTROL CENTER |
| R24 MCC C14 | 1 | MOTOR CONTROL CENTER |
| R24 MCC C17 | 1 | MOTOR CONTROL CENTER |
| R24 MCC D10 | 2 | MOTOR CONTROL CENTER |
| R24 MCC D11 | 2 | MOTOR CONTROL CENTER |
| R24 MCC D12 | 2 | MOTOR CONTROL CENTER |
| R24 MCC D14 | 2 | MOTOR CONTROL CENTER |
| R24 MCC D17 | 2 | MOTOR CONTROL CENTER |
| R24 MCC E10 | 3 | MOTOR CONTROL CENTER |
| R24 MCC E11 | 3 | MOTOR CONTROL CENTER |
| R24 MCC E14 | 3 | MOTOR CONTROL CENTER |
| R24 MCC E17 | 3 | MOTOR CONTROL CENTER |
| R42-P005A | 1 | 125 VDC NORM CHARGER |
| R42-P005B | 2 | 125 VDC NORM CHARGER |
| R42-P005C | 3 | 125 VDC NORM CHARGER |
| R42-P005D | 4 | 125 VDC NORM CHARGER |
| R42-P006A | 1 | 125 VDC NORM CHARGER |
| R42-P006B | 2 | 125 VDC NORM CHARGER |
| R42-P006C | 3 | 125 VDC NORM CHARGER |
| R42-P006D | 4 | 125 VDC NORM CHARGER |

## Table 7A-1 List of Equipment Interface with Essential MUX Signals (Continued)

| Device | Div | Description |
|---|---|---|
| R42-P007A | 1 | 125 VDC CNTR DIST BD |
| R42-P007B | 2 | 125 VDC CNTR DIST BD |
| R42-P007C | 3 | 125 VDC CNTR DIST BD |
| R42-P007D | 4 | 125 VDC CNTR DIST BD |
| R42-P008A | 1,2 | 125 VDC STBY CHARGER |
| R42-P008B | 1,3 | 125 VDC STBY CHARGER |
| R43-C201A | 1 | COMPRESSOR |
| R43-C201B | 2 | COMPRESSOR |
| R43-C201C | 3 | COMPRESSOR |
| R43-C202A | 1 | COMPRESSOR |
| R43-C202B | 2 | COMPRESSOR |
| R43-C202C | 3 | COMPRESSOR |
| R43-C401A | 1 | LUBE OIL PUMP |
| R43-C401B | 2 | LUBE OIL PUMP |
| R43-C401C | 3 | LUBE OIL PUMP |
| R43-DPS091A | 1 | DIFF PRESS SWITCH |
| R43-DPS091B | 2 | DIFF PRESS SWITCH |
| R43-DPS091C | 3 | DIFF PRESS SWITCH |
| R43-J001A | 1 | DIESEL GENERATOR |
| R43-J001B | 2 | DIESEL GENERATOR |
| R43-J001C | 3 | DIESEL GENERATOR |
| R43-LIS191A | 1 | LEVEL IND SWITCH |
| R43-LIS191B | 2 | LEVEL IND SWITCH |
| R43-LIS191C | 3 | LEVEL IND SWITCH |
| R43-LS142A | 1 | LEVEL SWITCH |
| R43-LS142B | 2 | LEVEL SWITCH |
| R43-LS142C | 3 | LEVEL SWITCH |
| R43-LS395A | 1 | LEVEL SWITCH |
| R43-LS395B | 2 | LEVEL SWITCH |
| R43-LS395C | 3 | LEVEL SWITCH |
| R43-P001A | 1 | DG(A) CONTROL PNL (A) |
| R43-P001B | 2 | DG(B) CONTROL PNL (A) |
| R43-P001C | 3 | DG(C) CONTROL PNL (A) |
| R43-P002A | 1 | DG(A) SCT PANEL |
| R43-P002B | 2 | DG(B) SCT PANEL |
| R43-P002C | 3 | DG(C) SCT PANEL |

## Table 7A-1 List of Equipment Interface with Essential MUX Signals (Continued)

| Device | Div | Description |
|---|---|---|
| R43-P003A | 1 | DG(A) CONTROL PNL (B) |
| R43-P003B | 2 | DG(B) CONTROL PNL (B) |
| R43-P003C | 3 | DG(C) CONTROL PNL (B) |
| R46-J002A1 | 1 | VITAL DIST PNL A1 |
| R46-J002B1 | 2 | VITAL DIST PNL B1 |
| R46-J002C1 | 3 | VITAL DIST PNL C1 |
| R46-J002D1 | 4 | VITAL DIST PNL D1 |
| R46-P001A | 1 | VITAL CVCF A |
| R46-P001B | 2 | VITAL CVCF B |
| R46-P001C | 3 | VITAL CVCF C |
| R46-P001D | 4 | VITAL CVCF D |
| T22-B001B | 2 | DIFF PRESS TRANSMITTER |
| T22-B001C | 3 | DIFF PRESS TRANSMITTER |
| T22-C001B | 2 | PROCESS FAN (B) |
| T22-C001C | 3 | PROCESS FAN (C) |
| T22-C002B | 2 | COOLING FAN (B) |
| T22-C002C | 3 | COOLING FAN (C) |
| T22-D001B | 2 | FILTER TRAIN UNIT (B) |
| T22-D001C | 3 | FILTER TRAIN UNIT (C) |
| T22-DPT003 | 3 | DIFF PRESS TRANSMITTER |
| T22-DPT007 | 3 | DIFF PRESS TRANSMITTER |
| T22-DPT008 | 3 | DIFF PRESS TRANSMITTER |
| T22-DPT012 | 3 | DIFF PRESS TRANSMITTER |
| T22-DPT017 | 3 | DIFF PRESS TRANSMITTER |
| T22-DPT021A | 1 | DIFF PRESS TRANSMITTER |
| T22-DPT021B | 2 | DIFF PRESS TRANSMITTER |
| T22-DPT021C | 3 | DIFF PRESS TRANSMITTER |
| T22-DPT021D | 4 | DIFF PRESS TRANSMITTER |
| T22-DPT022 | 2 | DIFF PRESS TRANSMITTER |
| T22-DPT027 | 2 | DIFF PRESS TRANSMITTER |
| T22-DPT103 | 2 | DIFF PRESS TRANSMITTER |
| T22-DPT107 | 2 | DIFF PRESS TRANSMITTER |
| T22-DPT108 | 2 | DIFF PRESS TRANSMITTER |
| T22-F002B | 2 | MO BUTTERFLY VALVE |
| T22-F002C | 3 | MO BUTTERFLY VALVE |
| T22-F004B | 2 | MO BUTTERFLY VALVE |

## Table 7A-1 List of Equipment Interface with Essential MUX Signals (Continued)

| Device | Div | Description |
|---|---|---|
| T22-F004C | 3 | MO BUTTERFLY VALVE |
| T22-F005B | 2 | MO BUTTERFLY VALVE |
| T22-F005C | 3 | MO BUTTERFLY VALVE |
| T22-FT018B | 2 | FLOW TRANSMITTER |
| T22-FT018C | 3 | FLOW TRANSMITTER |
| T22-H001C1 | 3 | PRE SPACE HEATER |
| T22-H001C2 | 3 | PRE SPACE HEATER |
| T22-H001C3 | 3 | AFTER SPACE HEATER |
| T22-H001C4 | 3 | AFTER SPACE HEATER |
| T22-H001B1 | 2 | PRE SPACE HEATER |
| T22-H001B2 | 2 | PRE SPACE HEATER |
| T22-H001B3 | 2 | AFTER SPACE HEATER |
| T22-H001B4 | 2 | AFTER SPACE HEATER |
| T22-LS004B | 2 | LEVEL SWITCH |
| T22-LS004C | 3 | LEVEL SWITCH |
| T22-LS029C | 3 | LEVEL SWITCH |
| T22-LS029B | 2 | LEVEL SWITCH |
| T22-ME011B | 2 | MOISTURE ELEMENT |
| T22-ME011C | 3 | MOISTURE ELEMENT |
| T22-ME012B | 2 | MOISTURE ELEMENT |
| T22-ME012C | 3 | MOISTURE ELEMENT |
| T22-MT011B | 2 | MOISTURE TRANSMITTER |
| T22-MT011C | 3 | MOISTURE TRANSMITTER |
| T22-MT012B | 2 | MOISTURE TRANSMITTER |
| T22-MT012C | 3 | MOISTURE TRANSMITTER |
| T22-POE001B | 2 | POSITION ELEMENT |
| T22-POE001C | 3 | POSITION ELEMENT |
| T22-TE002B | 2 | TEMP ELEMENT |
| T22-TE002C | 3 | TEMP ELEMENT |
| T22-TE010B | 2 | TEMP ELEMENT |
| T22-TE010C | 3 | TEMP ELEMENT |
| T22-TE013B | 2 | TEMP ELEMENT |
| T22-TE013C | 3 | TEMP ELEMENT |
| T22-TE014B | 2 | TEMP ELEMENT |
| T22-TE014C | 3 | TEMP ELEMENT |
| T22-TE016B | 2 | TEMP ELEMENT |

## Table 7A-1 List of Equipment Interface with Essential MUX Signals (Continued)

| Device | Div | Description |
|---|---|---|
| T22-TE016C | 3 | TEMP ELEMENT |
| T22-TS005B | 2 | TEMP SWITCH |
| T22-TS005C | 3 | TEMP SWITCH |
| T22-TS009B | 2 | TEMP SWITCH |
| T22-TS009C | 3 | TEMP SWITCH |
| T22-TS013B | 2 | TEMP SWITCH |
| T22-TS013C | 3 | TEMP SWITCH |
| T22-TS015B | 2 | TEMP ELEMENT |
| T22-TS015C | 3 | TEMP ELEMENT |
| T31-F001 | 1 | AO VALVE |
| T31-F002 | 2 | AO VALVE |
| T31-F003 | 2 | AO VALVE |
| T31-F004 | 2 | AO VALVE |
| T31-F005 | 2 | AO VALVE |
| T31-F006 | 2 | AO VALVE |
| T31-F007 | 2 | AO VALVE |
| T31-F008 | 1 | AO VALVE |
| T31-F009 | 1 | AO VALVE |
| T31-F010 | 1 | AO VALVE |
| T31-F011 | 3 | AO VALVE |
| T31-F025 | 1 | AO VALVE |
| T31-F039 | 1 | AO VALVE |
| T31-F040 | 2 | AO VALVE |
| T31-F041 | 2 | AO VALVE |
| T31-F044A-H | 1 | POSITION SWITCH |
| T31-F044A-H | 2 | POSITION SWITCH |
| T31-F731 | 1 | SO VALVE |
| T31-F733A | 1 | SO VALVE |
| T31-F733B | 1 | SO VALVE |
| T31-F735A | 1 | SO VALVE |
| T31-F735B | 2 | SO VALVE |
| T31-F735C | 3 | SO VALVE |
| T31-F735D | 4 | SO VALVE |
| T31-F737A | 1 | SO VALVE |
| T31-F737B | 1 | SO VALVE |
| T31-F739A | 1 | SO VALVE |

## Table 7A-1 List of Equipment Interface with Essential MUX Signals (Continued)

| Device | Div | Description |
|---|---|---|
| T31-F739B | 2 | SO VALVE |
| T31-F739C | 3 | SO VALVE |
| T31-F739D | 4 | SO VALVE |
| T31-F741A | 1 | SO VALVE |
| T31-F741B | 2 | SO VALVE |
| T31-F741C | 3 | SO VALVE |
| T31-F741D | 4 | SO VALVE |
| T31-F743A | 1 | SO VALVE |
| T31-F743B | 2 | SO VALVE |
| T31-F745A | 1 | SO VALVE |
| T31-F745B | 2 | SO VALVE |
| T31-F801A | 1 | SO VALVE |
| T31-F801B | 2 | SO VALVE |
| T31-F803A | 1 | SO VALVE |
| T31-F803B | 2 | SO VALVE |
| T31-F805A | 1 | SO VALVE |
| T31-F805B | 2 | SO VALVE |
| T31-LT058A | 1 | LEVEL TRANSMITTER |
| T31-LT058B | 2 | LEVEL TRANSMITTER |
| T31-LT058C | 3 | LEVEL TRANSMITTER |
| T31-LT058D | 4 | LEVEL TRANSMITTER |
| T31-LT059A | 1 | LEVEL TRANSMITTER |
| T31-LT059B | 2 | LEVEL TRANSMITTER |
| T31-LT100A | 1 | LEVEL TRANSMITTER |
| T31-LT100B | 2 | LEVEL TRANSMITTER |
| T49-C001B | 2 | BLOWER |
| T49-C001C | 3 | BLOWER |
| T49-D002B | 2 | HEATER |
| T49-D002C | 3 | HEATER |
| T49-F001B | 2 | MO GATE VALVE |
| T49-F001C | 3 | MO GATE VALVE |
| T49-F002A | 1 | AO GATE VALVE |
| T49-F002A | 3 | AO GATE VALVE |
| T49-F002E | 1 | AO GATE VALVE |
| T49-F002E | 2 | AO GATE VALVE |
| T49-F003B | 2 | MO GLOBE VALVE |

## Table 7A-1 List of Equipment Interface with Essential MUX Signals (Continued)

| Device | Div | Description |
|---|---|---|
| T49-F003C | 3 | MO GLOBE VALVE |
| T49-F004B | 2 | MO GLOBE VALVE |
| T49-F004C | 3 | MO GLOBE VALVE |
| T49-F006A | 1 | AO GATE VALVE |
| T49-F006A | 3 | AO GATE VALVE |
| T49-F006E | 1 | AO GATE VALVE |
| T49-F006E | 2 | AO GATE VALVE |
| T49-F007B | 2 | MO GATE VALVE |
| T49-F007C | 3 | MO GATE VALVE |
| T49-F008B | 2 | MO GATE VALVE |
| T49-F008C | 3 | MO GATE VALVE |
| T49-F009B | 2 | MAN OPER GLOBE VALVE |
| T49-F009C | 3 | MAN OPER GLOBE VALVE |
| T49-F010B | 2 | MO GLOBE VALVE |
| T49-F010C | 3 | MO GLOBE VALVE |
| T49-F013B | 2 | MAN OPER GATE VALVE |
| T49-F013C | 3 | MAN OPER GATE VALVE |
| T49-F014B | 2 | MAN OPER GATE VALVE |
| T49-F014C | 3 | MAN OPER GATE VALVE |
| T49-FT002B | 2 | FLOW TRANSMITTER |
| T49-FT002C | 3 | FLOW TRANSMITTER |
| T49-FT004B | 2 | FLOW TRANSMITTER |
| T49-FT004C | 3 | FLOW TRANSMITTER |
| T49-PT003B | 2 | PRESS TRANSMITTER |
| T49-PT003C | 3 | PRESS TRANSMITTER |
| T49-TE001B | 2 | TEMP ELEMENT |
| T49-TE001C | 3 | TEMP ELEMENT |
| T49-TE005B | 2 | TEMP ELEMENT |
| T49-TE005C | 3 | TEMP ELEMENT |
| T49-TE006B-1 | 2 | TEMP ELEMENT |
| T49-TE006C-1 | 3 | TEMP ELEMENT |
| T49-TE007B-1 | 2 | TEMP ELEMENT |
| T49-TE007C-1 | 3 | TEMP ELEMENT |
| T49-TE008B-1 | 2 | TEMP ELEMENT |
| T49-TE008C-1 | 3 | TEMP ELEMENT |
| T49-TE009B-1 | 2 | TEMP ELEMENT |

## Table 7A-1 List of Equipment Interface with Essential MUX Signals (Continued)

| Device | Div | Description |
|---|---|---|
| T49-TE009C-1 | 3 | TEMP ELEMENT |
| T49-TE010B-1 | 2 | TEMP ELEMENT |
| T49-TE010C-1 | 3 | TEMP ELEMENT |
| T49-TE011B-1 | 2 | TEMP ELEMENT |
| T49-TE011C-1 | 3 | TEMP ELEMENT |
| T53-TE001A | 1 | TEMPERATURE ELEMENT |
| T53-TE001C | 3 | TEMPERATURE ELEMENT |
| T53-TE001E | 1 | TEMPERATURE ELEMENT |
| T53-TE001G | 3 | TEMPERATURE ELEMENT |
| T53-TE001J | 1 | TEMPERATURE ELEMENT |
| T53-TE001L | 3 | TEMPERATURE ELEMENT |
| T53-TE001N | 1 | TEMPERATURE ELEMENT |
| T53-TE001R | 3 | TEMPERATURE ELEMENT |
| T53-TE002B | 2 | TEMPERATURE ELEMENT |
| T53-TE002D | 4 | TEMPERATURE ELEMENT |
| T53-TE002F | 2 | TEMPERATURE ELEMENT |
| T53-TE002H | 4 | TEMPERATURE ELEMENT |
| T53-TE002K | 2 | TEMPERATURE ELEMENT |
| T53-TE002M | 4 | TEMPERATURE ELEMENT |
| T53-TE002P | 2 | TEMPERATURE ELEMENT |
| T53-TE002S | 4 | TEMPERATURE ELEMENT |
| T53-TE003B | 2 | TEMPERATURE ELEMENT |
| T53-TE003D | 4 | TEMPERATURE ELEMENT |
| T53-TE003F | 2 | TEMPERATURE ELEMENT |
| T53-TE003H | 4 | TEMPERATURE ELEMENT |
| T53-TE003K | 2 | TEMPERATURE ELEMENT |
| T53-TE003M | 4 | TEMPERATURE ELEMENT |
| T53-TE003P | 2 | TEMPERATURE ELEMENT |
| T53-TE003S | 4 | TEMPERATURE ELEMENT |
| T53-TE004A | 1 | TEMPERATURE ELEMENT |
| T53-TE004C | 3 | TEMPERATURE ELEMENT |
| T53-TE004E | 1 | TEMPERATURE ELEMENT |
| T53-TE004G | 3 | TEMPERATURE ELEMENT |
| T53-TE004J | 1 | TEMPERATURE ELEMENT |
| T53-TE004L | 3 | TEMPERATURE ELEMENT |
| T53-TE004N | 1 | TEMPERATURE ELEMENT |

## Table 7A-1 List of Equipment Interface with Essential MUX Signals (Continued)

| Device | Div | Description |
|---|---|---|
| T53-TE004R | 3 | TEMPERATURE ELEMENT |
| T53-TE005A | 1 | TEMPERATURE ELEMENT |
| T53-TE005C | 3 | TEMPERATURE ELEMENT |
| T53-TE005E | 1 | TEMPERATURE ELEMENT |
| T53-TE005G | 3 | TEMPERATURE ELEMENT |
| T53-TE005J | 1 | TEMPERATURE ELEMENT |
| T53-TE005L | 3 | TEMPERATURE ELEMENT |
| T53-TE005N | 1 | TEMPERATURE ELEMENT |
| T53-TE005R | 3 | TEMPERATURE ELEMENT |
| T53-TE006B | 2 | TEMPERATURE ELEMENT |
| T53-TE006D | 4 | TEMPERATURE ELEMENT |
| T53-TE006F | 2 | TEMPERATURE ELEMENT |
| T53-TE006H | 4 | TEMPERATURE ELEMENT |
| T53-TE006K | 2 | TEMPERATURE ELEMENT |
| T53-TE006M | 4 | TEMPERATURE ELEMENT |
| T53-TE006P | 2 | TEMPERATURE ELEMENT |
| T53-TE006S | 4 | TEMPERATURE ELEMENT |
| T53-TE007B | 2 | TEMPERATURE ELEMENT |
| T53-TE007D | 4 | TEMPERATURE ELEMENT |
| T53-TE007F | 2 | TEMPERATURE ELEMENT |
| T53-TE007H | 4 | TEMPERATURE ELEMENT |
| T53-TE007K | 2 | TEMPERATURE ELEMENT |
| T53-TE007M | 4 | TEMPERATURE ELEMENT |
| T53-TE007P | 2 | TEMPERATURE ELEMENT |
| T53-TE007S | 4 | TEMPERATURE ELEMENT |
| T53-TE008A | 1 | TEMPERATURE ELEMENT |
| T53-TE008C | 3 | TEMPERATURE ELEMENT |
| T53-TE008E | 1 | TEMPERATURE ELEMENT |
| T53-TE008G | 3 | TEMPERATURE ELEMENT |
| T53-TE008J | 1 | TEMPERATURE ELEMENT |
| T53-TE008L | 3 | TEMPERATURE ELEMENT |
| T53-TE008N | 1 | TEMPERATURE ELEMENT |
| T53-TE008R | 3 | TEMPERATURE ELEMENT |
| U41-C201A | 1 | DG(A) SUPPLY FAN (A) |
| U41-C201E | 1 | DG(A) SUPPLY FAN (E) |
| U41-C202A | 1 | DG(A) EXHAUST FAN (A) |

## Table 7A-1 List of Equipment Interface with Essential MUX Signals (Continued)

| Device | Div | Description |
|---|---|---|
| U41-C202E | 1 | DG(A) EXHAUST FAN (E) |
| U41-C203A | 1 | DG(A) EMER SUPP FAN (A) |
| U41-C203E | 1 | DG(A) EMER SUPP FAN (E) |
| U41-C204B | 2 | DG(B) SUPPLY FAN (B) |
| U41-C204F | 2 | DG(B) SUPPLY FAN (F) |
| U41-C205B | 2 | DG(B) EXHAUST FAN (B) |
| U41-C205F | 2 | DG(B) EXHAUST FAN (F) |
| U41-C206B | 2 | DG(B) EMER SUPP FAN (B) |
| U41-C206F | 2 | DG(B) EMER SUPP FAN (F) |
| U41-C207C | 3 | DG(C) SUPPLY FAN (C) |
| U41-C207G | 3 | DG(C) SUPPLY FAN (G) |
| U41-C208C | 3 | DG(C) EXHAUST FAN (C) |
| U41-C208G | 3 | DG(C) EXHAUSR FAN (G) |
| U41-C209C | 3 | DG(C) EMER SUPP FAN (C) |
| U41-C209G | 3 | DG(C) EMER SUPP FAN (G) |
| U41-C601B | 2 | MCR SUPPLY FAN (B) |
| U41-C601F | 2 | MCR SUPPLY FAN (F) |
| U41-C602B | 2 | MCR EXHAUST FAN (B) |
| U41-C602F | 2 | MCR EXHAUST FAN (F) |
| U41-C603B | 2 | MCR RECIRC SUPP FAN (B) |
| U41-C603F | 2 | MCR RECIRC SUPP FAN (F) |
| U41-C604A | 1 | EMER EQ FAN(A) ZONE(A) |
| U41-C604E | 1 | EMER EQ FAN(B) ZONE(A) |
| U41-C605A | 1 | EM EQ EX FAN(A) ZONE(A) |
| U41-C605E | 1 | EM EQ EX FAN(B) ZONE(A) |
| U41-C606B | 2 | EMER EQ FAN(A) ZONE(B) |
| U41-C606F | 2 | EMER EQ FAN(B) ZONE(B) |
| U41-C607B | 2 | EM EQ EX FAN(A) ZONE(B) |
| U41-C607F | 2 | EM EQ EX FAN(B) ZONE(B) |
| U41-C608C | 3 | EMER EQ FAN(A) ZONE(C) |
| U41-C608G | 3 | EMER EQ FAN (B) ZONE(C) |
| U41-C609C | 3 | EM EQ EX FAN(A) ZONE(C) |
| U41-C609G | 3 | EM EQ EX FAN(B) ZONE(C) |
| U41-C621C | 3 | MCR SUPPLY FAN (C) |
| U41-C621G | 3 | MCR SUPPLY FAN (G) |
| U41-C622C | 3 | MCR SUPPLY FAN (C) |
| U41-C622G | 3 | MCR SUPPLY FAN (G |

## Table 7A-1 List of Equipment Interface with Essential MUX Signals (Continued)

| Device | Div | Description |
|---|---|---|
| U41-C623C | 3 | MCR RECIRC SUPP FAN (C) |
| U41-C623G | 3 | MCR RECIRC SUPP FAN (G) |
| U41-D101 | 1 | RCIC PUMP ROOM HVH |
| U41-D102 | 3 | HPCF PUMP (C) ROOM HVH |
| U41-D103 | 1 | RHR PUMP (A) ROOM HVH |
| U41-D104 | 3 | RHR PUMP (C) ROOM HVH |
| U41-D105 | 2 | RHR PUMP (B) ROOM HVH |
| U41-D106 | 2 | HPCF PUMP (B) ROOM HVH |
| U41-D107 | 3 | FCS ROOM (A) HVH |
| U41-D108 | 2 | FCS ROOM (B) HVH |
| U41-D109 | 1 | FPC PUMP (A) ROOM HVH |
| U41-D110 | 2 | FPC PUMP (B) ROOM HVH |
| U41-D111 | 3 | SGTS ROOM HVH (C) |
| U41-D112 | 2 | SGTS ROOM HVH (B) |
| U41-D113 | 1 | CAMS (A) ROOM HVH |
| U41-D114 | 2 | CAMS (B) ROOM HVH |
| U41-F001A | 1 | AO VLV - R/A SUP ISO VLV |
| U41-F001B | 2 | AO VLV - R/A SUP ISO VLV |
| U41-F002A | 1 | AO VLV - R/A EXH ISO (A) |
| U41-F002B | 2 | AO VLV - R/A EXH ISO (B) |
| U41-F003A | 1 | MO VALVE |
| U41-F003B | 2 | MO VALVE |
| U41-F003C | 3 | MO VALVE |
| U41-F004A | 1 | MO VALVE |
| U41-F004B | 2 | MO VALVE |
| U41-F004C | 3 | MO VALVE |
| U41-F005A | 1 | MO VALVE |
| U41-F005B | 2 | MO VALVE |
| U41-F005C | 3 | MO VALVE |
| U41-TE052 | 1 | TEMP ELEMENT |
| U41-TE056 | 2 | TEMP ELEMENT |
| U41-TE060 | 3 | TEMP ELEMENT |
| U41-TE103B | 2 | TEMP ELEMENT |
| U41-TE103C | 3 | TEMP ELEMENT |

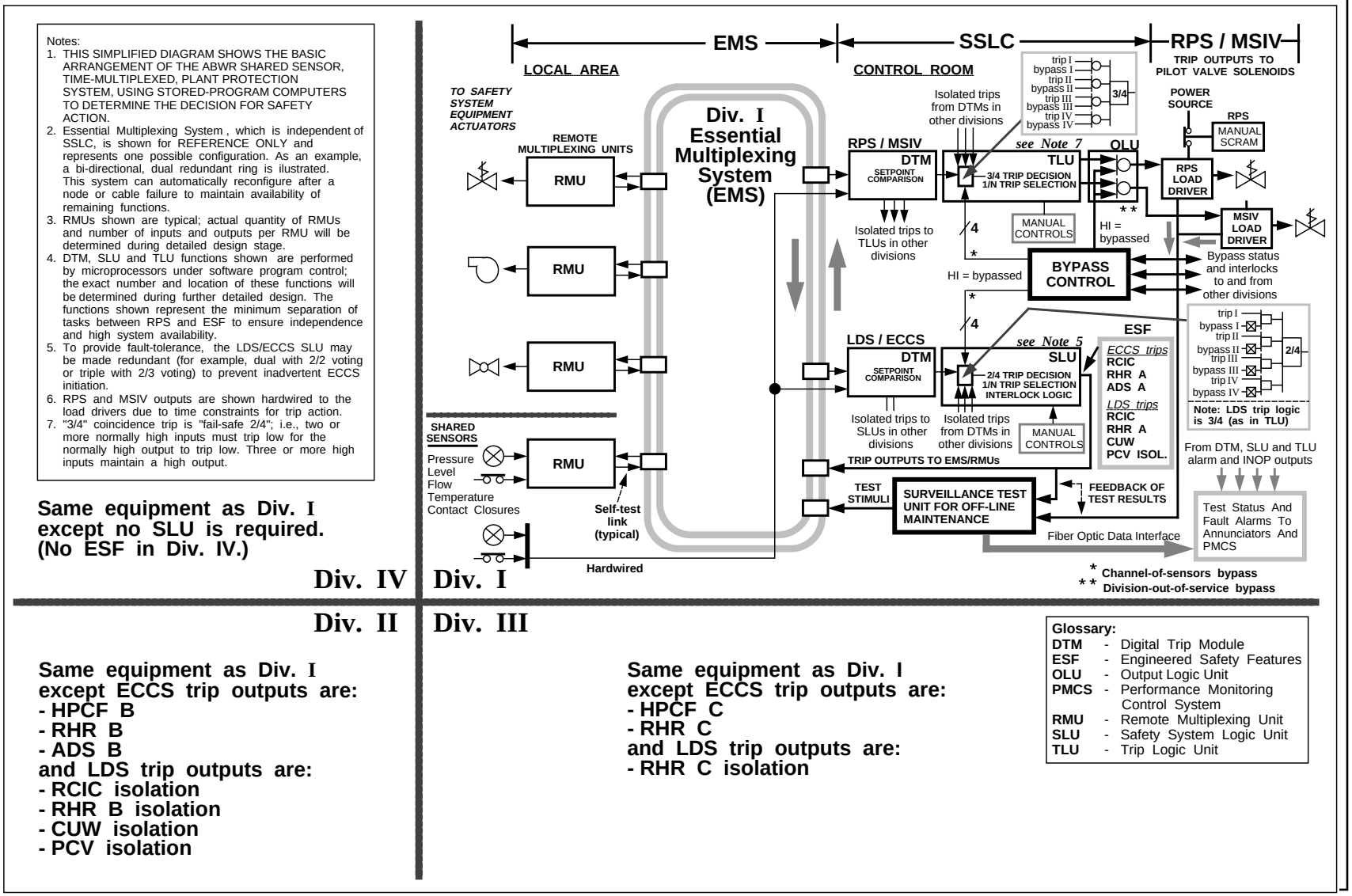



**Figure 7A-1 Safety System Logic and Control (SSLC)**

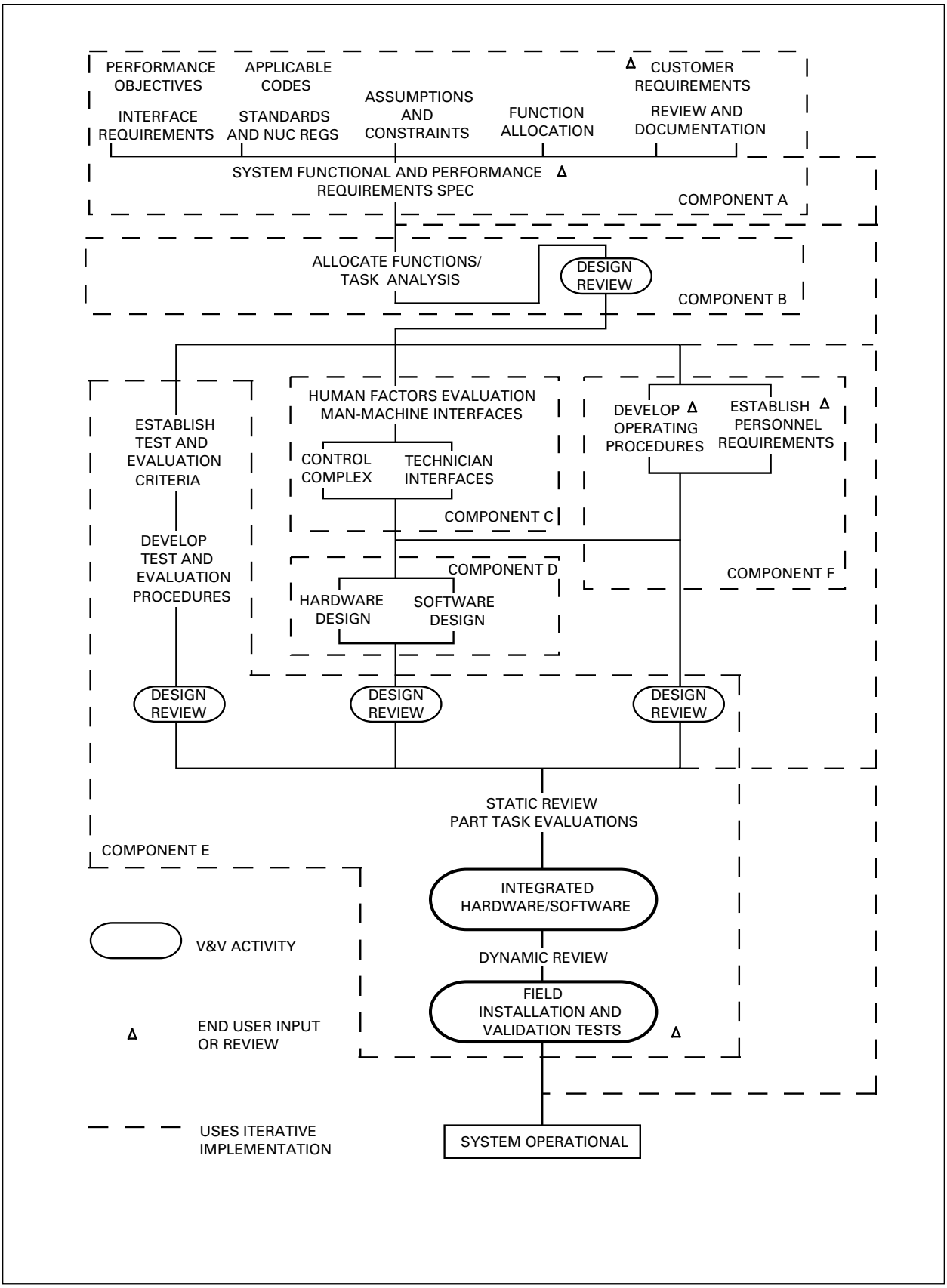



**Figure 7A-2 Structure for Control and Instrumentation System Design**

# 7B Implementation Requirements for Hardware/Software Development

This section defines the requirements to be met by the hardware and software development implementation activities that are to be made available for review by the NRC.

## 7B.1 Software Management Plan

[*The Software Management Plan shall define:*

*(a) the organization and responsibilities for development of the software design; the procedures to be used in the software development; the interrelationships between software design activities; and the methods for conducting software safety analyses.*

*Within the defined scope and content of the Software Management Plan, accepted methods and procedures for the above activities are presented in the following documents:*

***(i) [IEEE 730, Standard for Software Quality Assurance Plans, Section 3.4;***

***(ii) ASME NQA-2a, Part 2.7, Quality Assurance Requirements of Computer Software for Nuclear Facility Application;***

***(iii) ANSI/IEEE-ANS-7-4.3.2, Application Criteria for Digital Computers in Safety Systems for Nuclear Facilities (to be replaced by the issued version of P 7-4.3.2, "Standard Criteria for Digital Computers Used in Safety Systems of Nuclear Power Generation Stations");***

***(iv) IEC 880, Software for computers in the safety systems of nuclear power stations, Section 3.1;***

***(v) IEEE 1228 (draft), Standard for Software Safety Plans;***

***(vi) IEEE 1012, Standard for Software Verification and Validation Plans, Section 3.5;***

***(vii) IEEE 830, Guide to Software Requirements Specifications, Section 5;***

***(viii) IEEE 1042, Guide to Software Configuration Management.]****

*Note that within the set of documents listed above, differences may exist regarding specific methods and criteria applicable to the Software Management Plan. In situations where such differences exist, all of the methods and criteria presented within those documents are considered to be equally appropriate and valid and, therefore, any of the above listed documents may be selected as the basis for elements of the SMP.*

* See Sections 7A.1(2) and 7A.1(1).

*(b) that the software safety analyses to be conducted for safety-related software applications shall:*

*(i) identify software requirements having safety-related implications;*

*(ii) document the identified safety-critical software requirements in the software requirements specification for the design;*

*(iii) incorporate in to the software design the safety-critical software functions specified in the software requirements specification;*

*(iv) identify in the coding and test of the developed software, those software modules which are safety-critical;*

*(v) evaluate the performance of the developed safety-critical software modules when operated within the constraints imposed by the established system requirements, software design, and computer hardware requirements;*

*(vi) evaluate software interfaces of safety-critical software modules;*

*(vii) perform equipment integration and validation testing that demonstrate that safety-related functions identified in the design input requirements are operational.*

*(c) the software engineering process, which is composed of the following life-cycle phases:*

*(i) Planning*

*(ii) Design Definition*

*(iii) Software Design*

*(iv) Software Coding*

*(v) Integration*

*(vi) Validation*

*(vii) Change control*

*(d) the Planning phase design activities, which shall address the following system design requirements and software development plans:*

*(i) Software Management Plan*

*(ii) Software Configuration Management Plan*

*(iii) Verification and Validation Plan*

*(iv) Equipment design requirements*

*(v) Safety analysis of design requirements*

*(vi) disposition of design and/or documentation nonconformances identified during this phase*

*(e) the Design Definition phase design activities, which shall address the development of the following implementing equipment design and configuration requirements:*

*(i) equipment schematic;*

*(ii) equipment hardware and software performance specification;*

*(iii) equipment user's manual;*

*(iv) data communications protocol;*

*(v) safety analysis of the developed design definition;*

*(vi) disposition of design and/or documentation nonconformances identified during this phase.*

*(f) the Software Design phase, which shall address the design of the software architecture and program structure elements, and the definition of software module functions:*

*(i) Software Design Specification;*

*(ii) safety analysis of the software design;*

*(iii) disposition of design and/or documentation nonconformances identified during this phase.*

*(g) the Software Coding phase, which shall address the following software coding and testing activities of individual software modules:*

*(i) software source code;*

*(ii) software module test reports;*

*(iii) safety analysis of the software coding;*

*(iv) disposition of nonconformances identified in this phase's design documentation and test results.*

*(h) the Integration phase, which shall address the following equipment testing activities that evaluates the performance of the software when installed in hardware prototypical of that defined in the Design Definition phase:*

*(i) integration test reports;*

*(ii) safety analysis of the integration test results;*

*(iii) disposition of nonconformances identified in this phase's design documentation and test results.*

*(i) the Validation phase, which comprises the development and implementation of the following documented test plans and procedures:*

*(i) validation test plans and procedures;*

*(ii) validation test reports;*

*(iii) description of as-tested software;*

*(iv) safety analysis of the validation test results;*

*(v) disposition of nonconformances identified in this phase's design documentation and test results;*

*(vi) software change control procedures.*

*(j) the Change Control phase, which begins with the completion of validation testing, and addresses changes to previously validated software and the implementation of the established software change control procedures.*

## 7B.2 Configuration Management Plan

*The Configuration Management Plan shall define:*

*(a) the specific product or system scope to which it is applicable, the organizational responsibilities for software configuration management, and methods to be applied to:*

*(i) identify design interfaces;*

*(ii) produce software design documentation;*

*(iii) process changes to design interface documentation and software design documentation;*

*(iv) process corrective actions to resolve deviations identified in software design and design documentation, including notification to end user of errors discovered in software development tools or other software;*

*(v) maintain status of design interface documentation and developed software design documentation;*

*(vi) designate and control software revision status. Such methods shall require that software code listings present direct indication of the software code revision status.*

*Within the defined scope and content of the Configuration Management Plan, accepted methods and procedures for the above activities are presented in the following documents:*

***(i) [IEEE 1042, Guide to Software Configuration Management;***

***(ii) IEEE 828, Standard for Software Configuration Management Plans;***

***(iii) ANSI/IEEE-ANS-7-4.3.2, Application Criteria for Digital Computers in Safety Systems for Nuclear Facilities (to be replaced by the issued version***

***of P 7-4.3.2, "Standard Criteria for Digital Computers Used in Safety Systems of Nuclear Power Generation Stations");***

***(iv) IEC 880, Software for computers in the safety systems of nuclear power stations.]****

*Note that within the set of documents listed above, differences may exist regarding specific methods and criteria applicable to the Configuration Management Plan. In situations that such differences exist, all of the methods and criteria presented within those documents are considered to be equally appropriate and valid. Therefore, any of the above listed documents may be selected as the basis for elements of the CMP.*

*(b) methods for, and the sequencing of, reviews to evaluate the compliance of software design activities with the requirements of the CMP;*

*(c) the configuration management of tools (such as compilers) and software development procedures;*

*(d) methods for the dedication of commercial software for safety-related usage;*

*(e) methods for tracking error rates during software development, such as the use of software metrics;*

*(f) the methods for design record collection and retention.*

## 7B.3 Verification and Validation Plan

*The Verification and Validation Plan shall define:*

*(a) that baseline reviews of the software development process are to be conducted during each phase of the software development life cycle and the scope and methods to be used in the baseline reviews to evaluate the implemented design, design documentation, and compliance with the requirements of the Software Management Plan and Configuration Management Plan.*

*Within the defined scope and content of the Verification and Validation Plan, accepted methods and procedures for the above activities are presented in the following documents:*

***(i) [IEEE 1012, Standard for Software Verification and Validation Plans;***

***(ii) ANSI/IEEE-ANS-7-4.3.2, Application Criteria for Digital Computers in Safety Systems for Nuclear Facilities (to be replaced by the issued version***

* See Sections 7A.1(2) and 7A.1(1).

***of P 7-4.3.2, "Standard Criteria for Digital Computers Used in Safety Systems of Nuclear Power Generation Stations");***

***(iii) IEC 880, Software for computers in the safety systems of nuclear power stations.]****

*Note that within the set of documents listed above, differences may exist regarding specific methods and criteria applicable to the Verification and Validation Plan. In situations that such differences exist, all of the methods and criteria presented within those documents are considered to be equally appropriate and valid and, therefore, any of the above listed documents may be selected as the basis for elements of the V&VP.*

*(b) that verification shall be performed as a controlled and documented evaluation of the conformity of the developed design to the documented design requirements at each phase of baseline review.*

*(c) that the use of commercial software and commercial development tools for safety-related applications is a controlled and documented procedure.*

*(d) that validation shall be performed through controlled and documented testing of the developed software that demonstrates compliance of the software with the software requirements specifications.*

*(e) that for safety-related software, verification reviews and validation testing are to be conducted by personnel who are knowledgeable in the technologies and methods used in the design, but who did not develop the software design to be reviewed and tested.*

*(f) that for safety-related software, design verification reviews shall be conducted as part of the baseline reviews of the design material developed during the Planning through Integration phases of the software development life-cycle (as defined in Criterion 1b, above), and that validation testing shall be conducted as part of the baseline review of the Validation phase of the software development life-cycle.*

*(g) that validation testing shall be conducted per a documented test plan and procedure.*

*(h) that for non-safety-related software development, verification and validation shall be performed through design reviews conducted as part of the baseline reviews completed at the end of the phases in the software development life cycle. These design reviews shall be performed by personnel knowledgeable in the technologies and methods used in the design development.*

*(i) the products which shall result from the baseline reviews conducted at each phase of the software development life-cycle; and that the defined products of the baseline*

* See Sections 7A.1(2) and 7A.1(1).

*reviews and the V&V Plan shall be documented and maintained under configuration management.*

*(j) the methods for identification, closure, and documentation of design and/or design documentation nonconformances.*

*(k) that the software development is not complete until the specified verification and validation activities are complete and design documentation is consistent with the developed software.* ]*

### Completion of Software Development

Software development has been completed as defined in the SMP, CMP, and V&VP.

* See Section 7A.1(1).

# 7C Defense Against Common-Mode Failure in Safety-Related, Software-Based I&C Systems

## 7C.1 Introduction

The key feature of successful electronic instrumentation design for the ABWR is the application of state-of-the-art design techniques to modern, proven components that can be easily qualified to the required regulatory guidelines.

This is particularly true for microprocessors. Most of the effort in newer designs has been to do more functions at the highest possible speeds, which requires complex hardware and associated complex software. However, safety system logic in the ABWR uses only simple gating and interlock functions and does not require processing of complex algorithms. These functions can be very effectively accomplished by simpler microprocessors or microcontrollers, where high reliability and hardware simplicity become the key objectives.

Consistent with this philosophy is the use of state-of-the-art program design methods to achieve highly reliable software. These methods use simple data structures and modular, top-down programming to produce easily verifiable and testable programs that provide predictable performance.

This simplicity does not sacrifice the requirements for high speed data flow, fast time response, and good error detection, since modern microprocessors and microcontrollers fully support these requirements.

As described in Chapter 7 and Appendix 7A, the ABWR Safety System Logic and Control (SSLC) and Essential Multiplexing System (EMS) designs use programmable digital equipment to implement operating functions of the interfacing safety systems. A controlled process for software development and implementation is employed to ensure that the highest quality software is produced. The development process for safety-related software and its integration into read-only memory (ROM) as firmware includes a formal verification and validation (V&V) program, which is described in Appendices 7A and 7B. The V&V program, under control of the Software Management Plan, is applied to software that is developed for maximum reliability and efficiency, using a set of design techniques directed towards generating the simplest possible code to be used as firmware in dedicated, real-time microcontrollers

Despite the use of simple, reliable software; formal V&V; and built-in self-diagnostics, there is a concern that software design faults or other initiating events common to redundant, multi-divisional logic channels could disable significant portions of the plant's automatic standby safety functions (the reactor protection system and engineered safety features systems) at the moment when these functions are needed to

mitigate an accident. Mitigation of these common mode failures, as described in the following sections, is provided by the following diverse features:

(a) Manual scram and isolation by the operator in the main control room in response to diverse parameter indications.

(b) Core makeup water capability from the diverse feedwater, CRD, and condensate systems.

(c) Availability of manual high pressure injection capability.

(d) Long term shutdown capability provided in a conventionally hardwired, 2-division, analog remote shutdown system; local displays of process variables in RSS are continuously powered and so are available for monitoring at any time.

Note that random failures are mitigated by the divisional sensor channel and output trip channel bypass capability of SSLC. Either bypass places the remaining divisions in a 2-out-of-3 coincident logic condition such that another failure in a remaining division will not disable system operation.

## 7C.2 [*Design Techniques for Optimizing ABWR Safety-Related Hardware and Software*

*Before considering methods used to protect against common mode failure, several techniques that are employed to ensure system reliability by minimizing both random and common mode failure probabilities are outlined below:*

*(a) Design of self-test, surveillance, and calibration functions are performed as part of the initial design. These functions cannot successfully be added on to the basic functional hardware.*

*(b) The total amount of hardware is minimized to assure highest reliability.*

*(c) Microprocessors with minimal instruction sets and a simple operating system are used. The "lost" computing power is not needed and the limited instructions minimize inadvertent programming and operational errors. This aids in verification and validation and further enhances reliability.*

*(d) The highest quality, high precision components are used to gain reliability. Designs with these components minimize manual calibration, simplify reliability analysis, and maximize surveillance intervals.*

*(e) To improve maintainability, self-diagnostics are implemented to locate any problem to a single assembly.*

*(f) The man-machine interface is implemented such that the equipment is structured into small units, with enough diagnostics so that a user can repair equipment by*

*replacing modules and can operate the equipment by following straightforward instructions.*

*(g) The software design process specifies modular code*

*(h) Modules have one entry and one exit point and are written using a limited number of program constructs, as specified by* ***[DOD-STD-2167]****[*]

*(i) Code is segmented by system and function*

*(i) Program code for each safety system resides in independent modules which perform setpoint comparison, voting, and interlock logic*

*(ii) Code for calibration, signal I/O, self-diagnostics, and graphical displays is common to all systems*

*(iii) Fixed message formats are used for plant sensor data, equipment activation data and diagnostic data. Thus, corrupted messages are readily detected by error-detecting software in each digital instrument.*

*(j) Software design uses recognized defensive programming techniques, backed up by self-diagnostic software and hardware watchdog monitors*

*(k) A full-scope operating system is not used. The operating system for each instrument is a small, real-time kernel customized to perform only the required scheduling functions*

*(l) Software for control programs is permanently embedded as firmware in controller ROMs*

*(m) Commercial development tools and languages with a known history of successful applications in similar designs are used for software development.*

*(n) Automated software tools are used to aid in verification and validation*

*The most important factor, however, in implementing reliable software is the quality of the design and requirements specifications. These documents are also controlled under the formal V&V program.*

## 7C.3 Defense Against Common-Mode Failure

*SSLC performs several simple, repetitive tasks continuously and simultaneously in four independent and redundant divisions of logic: setpoint comparison, 2-out-of-4 voting logic, interlock logic, I/O, and self-test. As a practical matter, the development of common software modules for many of these functions has several advantages in producing reliable programs:*

*(a) Promotes standardization and code reusability*

* See Sections 7A.1(2) and 7A.1(1).

(b) *Minimizes program design errors*

(c) *Minimizes timing differences among channels*

(d) *Reduces software life cycle cost*

(i) *Simplifies verification*

(ii) *Reduces maintenance costs*

(iii) *Simplifies future changes*

*A strong V&V program can reduce the probability of common mode failure to a very low level because the simple modules used in each division, although identical in some cases, can be thoroughly tested during the validation process. In addition to software V&V, however, SSLC contains several system level and functional level defenses against common mode failure, as follows:*

(1) *System Level Defenses Against Common Mode Failure*

(a) *Operational defenses*

(i) *Asynchronous operation of multiple protection divisions; timing signals are not exchanged among divisions*

(ii) *Automatic error checking on all multiplexed transmission paths. Only the last good data is used for logic processing unless a permanent fault is detected, thereby causing the channel to trip and alarm.*

(iii) *Daily operator cross-check of redundant sensor inputs, in addition to automatic cross-checking*

(iv) *Quarterly surveillance of trip functions (on-line with division bypass capability)*

(v) *Continuous self-test with alarm outputs in all system devices*

(b) *Functional Defenses*

(i) *Instantaneous, simultaneous, and undetected failure on a common mode error is unlikely*

(ii) *Automatic error detection permits graceful shutdown*

(iii) *Separation and independence protect against global effects (EMI, thermal, etc.)*

*The functional program logic in the SSLC controllers also provides protection against common mode failures, as follows:*

*(1) Functional Defenses Against Common Mode Software Failure*

*(a) Control programs are not completely identical in each division*

*(i) Interlock logic for ESF pumps and valves varies in each division*

*(ii) Each division has different quantities and types of inputs and outputs*

*(iii) Redundant sensors have data messages with unique identifications and time-tags in each division*

*(b) Modules that are identical are simple functions such as setpoint comparison and 2-out-of-4 voting that can be readily verified*

*(c) Multiplexing and other data transmission functions use standard, open protocols that are verified to industry standards and are also qualified to Class 1E standards*

*Due to this extensive diversity that exists at the protection system and plant levels, the use of hardware and software diversity among the redundant channels of the protection system was not considered practical for the following reasons:*

*(1) Diverse software is more error prone during development and does not guarantee that the resulting system will be error-free*

*(2) Diverse hardware and software increases V&V and system integration costs*

*(3) The different types of hardware increases spares inventory*

*(4) Maintenance and surveillance require more time and attention because the diverse equipment may perform differently*

*(5) System revision costs are prohibitive because of additional V&V and documentation*

*(6) Performance of redundant channels may not be consistent*]*

## 7C.4 Common Mode Failure Analysis

**JANUARY, 1988 THROUGH SEPTEMBER, 1991**

As part of the initial efforts to support the licensing of the ABWR design in the U.S., GE provided the NRC staff with the results of evaluations demonstrating that the probability of a common-cause failure leading to the inability of the Safety System Logic and Control (SSLC) equipment to perform its safety functions was extremely low and,

* See Section 7A.1(1).

therefore, did not need to be considered further in the licensing process [see reference 7C-6(1)]. These analyses considered the defined SSLC configuration (e.g., 2-out-of-4 safety system logic and segmentation of functions performed with the multiple microprocessors of a safety division), system functions (e.g., automated self-test), and qualification of the equipment to the applicable standards (e.g., hardware qualification and software verification and validation (V&V).

During this initial period of ABWR design certification activities, the NRC staff was striving internally to define the methods that they should use to review and evaluate the acceptability of broad scope digital-based safety systems such as those which are incorporated into the ABWR design. Although the staff had some experience in reviewing and licensing individual systems and components that used advanced digital technologies (e.g., GE's NUMAC family of products), they had no experience in the review of broad scope integrated digital systems such as the SSLC design. In addition, the staff's past practice for the review of digital-based equipment was to review the actual implemented equipment hardware and software. For the ABWR design certification, the scope of their review specifically excluded the review of any particular implementation of equipment and, as a consequence, the NRC staff had no precedents to guide them in their review of ABWR licensing submittals regarding digital safety systems.

With the issuance of NRC paper SECY 91-292 (September 16, 1991), the staff indicated that they would require some type of I&C diversity in those plants that chose to implement broad scope digital systems in safety-related applications. The formal rationale presented by the staff indicated that the incorporation of such I&C diversity would provide additional "defense-in-depth" and that such an approach was already being taken in other countries (e.g., France).

**OCTOBER, 1991**

The NRC staff contracted with Lawrence Livermore National Laboratory (LLNL) to perform a "worst-case" common-mode failure (CMF) analysis of ABWR digital safety systems. LLNL defined "worst-case" to be an undetected, simultaneous, 4-division failure such that all safety actions are inhibited at the time that these actions are required by the coincident occurrence of a design basis event (accident or transient). The methodology to be used would be based on NUREG-0493 (1979).

**MARCH, 1992**

LLNL provided their first results to the NRC in March of 1992. Based upon the LLNL work, the staff formulated a position which included the requirement that "a set of safety grade displays and manual controls, independent of the computer system(s) and located in the main control room, shall be provided for system-level actuation and monitoring of critical safety function parameters..." and that "the displays and manual

controls shall be conventionally hardwired to as low a level in the system architecture as possible." [See reference 7C-6(2) for the final version of the LLNL report.]

**MAY, 1992**

GE responded with arguments to the staff that the LLNL analyses were based upon entirely incredible CMF sequences and, in addition, the analyses did not correctly reflect operator manual actions, the diverse capability of the Remote Shutdown System (RSS), or the operation of non-safety grade systems. In discussions with the staff, all of GE's arguments were accepted with the exception that the staff maintained the position that, for these evaluations of digital safety systems, the "worst-case" CMF sequences, like those modeled by LLNL, should be used as the basis of evaluation. GE committed to re-perform the basic analyses previously completed by LLNL using the following bases, in concurrence with the staff:

- The analyses presented in Chapter 15 of Tier 2 would be re-done with the modeling assumption that a worst-case postulated CMF of the digital safety systems would be considered concurrently with each of the individual design basis events.
- The analyses would be done using "realistic" modeling as opposed to standard "licensing basis" modeling, which can have significant additional margin inherent in the modeling.
- The analyses could take credit for non-safety controls and instrumentation if that equipment was independent of the postulated CMF in the digital safety systems.
- The analyses could take credit for operator actions at the RSS after one hour, but prior to that one hour period, all operator actions would be limited to those which could be performed in the main control room, using equipment that was independent of the postulated CMF.

**JUNE, 1992**

GE completed the evaluations and provided the results to the NRC staff. The evaluations took credit for the control room operation of the feedwater system and CRD hydraulic system to maintain RPV water level, and the use of a small set of "hardwired" displays and controls in the main control room for the purpose of the scram and containment isolation functions, which need to be accomplished in a relatively short time (i.e., at least within the first hour of the postulated event scenarios considered). To demonstrate that at least one hour of operation from only the control room was achievable, three of the most limiting scenarios were evaluated in detail, and the analyses were terminated after two hours of the scenario had been evaluated. The results of those evaluations (which were performed using the SAFR computer code) showed that even in the case where all operator actions are confined to just the control

room, the fuel peak clad temperature (PCT) could be maintained at less than 1204°C such that no additional hardwired functions beyond the small set considered in the analyses were needed. That small set of "hardwired" control and display functions was as follows:

CONTROLS

- Manual scram (included in standard design)
- Manual MSIV control (included in standard design)
- CUW line inboard isolation valve manual initiation (for CUW LOCA outside the primary containment)
- RCIC steamline inboard isolation valve manual initiation (for RCIC steam line break outside the primary containment)

DISPLAYS

- RPV water level
- RPV water level 3 alarm
- Drywell pressure
- Drywell pressure high alarm
- CUW line inboard isolation valve status
- RCIC steamline inboard isolation valve status
- MSIV status

Also in June of 1992, top GENE management met with the NRC commissioners and presented GE's position that the ABWR design already included adequate diversity and that the NRC staff's approach to requiring significant "hardwired" functions in the main control room was not technically justified.

**SEPTEMBER, 1992**

In a letter to the chairman of the NRC [see reference 7C-6(3)], the Advisory Committee on Reactor Safeguards (ACRS) rejected the NRC staff's position regarding the requirement for hardwired backup for the digital safety systems in the main control room (MCR). The ACRS position, which was consistent with the position that had been taken by GE and others in the nuclear industry, was that there are many potentially acceptable methods of implementing diversity that could be used to mitigate postulated

CMF of digital safety systems, and, thus, the NRC staff position which specifically required hardwired functions in the MCR was not technically justified.

**OCTOBER, 1992**

The staff modified its position on hardwired functions [see reference 7C-6(4)] and acknowledged that other methods (including diverse digital equipment) could be used to satisfy their requirement for mitigating postulated CMF of digital safety systems.

**DECEMBER, 1992**

The staff released the draft Final Safety Evaluation Report (FSER) on the ABWR. In that document, the staff presented their new list of diverse MCR displays and controls required for the ABWR. That list was essentially the same as the list developed by GE (see above) with one exception: The staff still required diverse HPCF manual initiation and flow indication in the MCR. In addition, the staff required that the feedwater system (FWS) be designed and tested to demonstrate high reliability. The rationale that the staff presented for requiring these additional diverse functions and capabilities was that, although the analyses submitted by GE in June 1992 had frequently taken credit for the operation of the FWS, the staff felt uncomfortable with placing such reliance on that system because past experience with single channel analog feedwater control system performance in U.S. plants had not been good.

**JANUARY, 1993**

In a meeting with the NRC staff, GE discussed the staff position presented in their draft FSER. GE argued that since the ABWR had incorporated a triplicated fault-tolerant architecture for the feedwater control system (FWCS), the reliability of feedwater control was significantly improved over past single-channel analog systems. The staff countered that, if GE was going to take credit for the feedwater system in the I&C common-mode failure analyses, they would then require that the FWCS be essentially designed and tested as though it were a safety-related system. In addition, the staff would still require that at least one division of HPCF manual initiation be provided in the MCR as redundant backup to the feedwater system.

During the January 1993 discussions, GE provided the staff with the results of new analyses that had been performed with the additional modeling assumption that the FWCS was assumed to have failed concurrent with the postulated initiating design basis event and the postulated worst-case CMF of the digital safety systems. In those analyses, only the operation of the CRD hydraulic system and the condensate system from the MCR were considered for the first two hours of the event. The results were still less than the 1204°C PCT limit. These analyses were used to demonstrate that even if the FWCS was assumed to have failed, there would still be adequate capability in the MCR (without hardwired manual HPCF initiation) to support operator actions to maintain the reactor

in a safe condition and provide sufficient time for an operator to move to the remote shutdown system to initiate core make-up systems from that location. The staff accepted these arguments and agreed that the requirements they had proposed regarding FWCS reliability and HPCF manual initiation capability could be deleted. However, the staff requested that three additional design basis events be evaluated using the same type of modeling assumptions, including the postulated concurrent failure of the FWCS. Together with the previous analyses, these additional evaluations would comprise a bounding set of Chapter 15 events regarding the consequences of common mode failure on the digital protection system.

**FEBRUARY, 1993**

GE submitted to the staff the results of the three additional analyses [see reference 7C-6(5)]. All results were again less than the defined 1204°C PCT limit.

## MARCH, 1993

The staff contacted GE to discuss some questions they had regarding the analyses previously provided by GE. The analyses included consideration of actions that would be taken by the operators in the MCR during the postulated events. These operator actions were defined based upon the ABWR Emergency Procedure Guidelines; the timing of these assumed operator actions was supported by operator performance test data from training simulators. The question raised by the Human Factors Branch of the NRC staff was basically: “How sensitive are the results of the GE analyses to the timing of the assumed operator actions?” More specifically, as an example, GE’s analyses modeled that the operator would initiate condensate system operation within 5 minutes after the RPV water level dropped below level 2. The NRC staff’s question was: “After how much longer would the analysis results still be acceptable?” GE agreed to re-perform the three most limiting analyses with the objective of trying to determine how long the operator could wait to take his first action. With the time margin for operator action quantified, and assuming this margin was sufficient, the staff agreed that the issue of I&C diversity would finally be closed with GE’s incorporation of the small set of MCR displays and controls presented above.

These final analyses were performed using the TRAC computer code. TRAC was used instead of the SAFR code employed in the previous analyses because the additional modeling assumption of a delayed operator action time causes a longer period of operation with a depressed RPV water level; the TRAC code was considered to do a better job of modeling these conditions. Note that the SAFR code is an approved Level 2 code for the performance of Design Basis LOCA analyses in which the ECCS initiates automatically and the period of core uncovery nominally lasts no longer than about 100 seconds. However, in these special analyses, the period of core uncovery would last for 1000 seconds or more and, therefore, were beyond the scope of the existing SAFR code

qualification. During the conduct of these evaluations using the TRAC code, it was determined that the previous analytical results obtained with the SAFR code were not correct and were non-conservative. Upon realization that the previous results were invalid, the entire set of six events previously analyzed in June 1992 were re-analyzed. The results of these TRAC analyses showed that the CRD hydraulic system and condensate system alone were not adequate to maintain the core within the 1204°C limit under the conditions postulated in those analyses. In order to maintain the core within the 1204°C limit for these postulated event scenarios, it was necessary to take credit for operation of one division of HPCF [see reference 7C-6(6)].

**MAY, 1993**

GE advised the staff that manual control of HPCF Loop C (Division III) and the display of HPCF Loop C flow would be added to the list presented above of hardwired displays and controls provided in the MCR. (Manual control of HPCF Loop B (Division II), with local display, is already provided at the RSS.)

**JUNE, 1993**

As of the week of June 7, 1993, the staff indicated that, with the addition of the hardwired HPCF manual control in the MCR, the issue of I&C diversity would be closed, pending the staff's final review of the results of the analyses that were re-done to incorporate manual HPCF initiation. Within the U.S. licensing material, manual HPCF Loop C initiation will be presented as a manual switch hardwired to a programmable logic controller (PLC) device that is independent of Safety System Logic and Control (SSLC) and the Essential Multiplexing System (EMS). SSLC and EMS will continue to provide the automatic software-based initiation logic for HPCF Loop C [see reference 7C-6(7)].

The SSLC design also uses hardwired control switches to perform manual system start of the other systems in ECCS. However, these switches are hardwired only from the operator's control station to the microprocessor logic in SSLC, where EMS then provides the transmission path for control signals from SSLC to the actuated devices. Control switch signals for individual control of pumps and valves are multiplexed from the operator's control station to SSLC and then through EMS as stated above.

**JULY, 1993**

The final NRC staff position on I&C diversity is stated in NRC document SECY-93-087, Section II.Q. This position has been approved by the NRC commissioners, with minor changes, in item 18 of a staff requirements memorandum (SRM), dated July 15, 1993. GE's design for safety-related I&C, as described in the above chronology and discussed in detail in the following section, fully meets the staff requirements.

## 7C.5 [DETAILS OF FINAL IMPLEMENTATION OF DIVERSITY IN ABWR PROTECTION SYSTEM

*To maintain protection system defense-in-depth in the presence of a postulated worst-case event (i.e., undetected, 4-division common mode failure of all communications or logic processing functions in conjunction with a large break LOCA), diversity is provided in the form of hardwired backup of reactor trip, diverse display of important process parameters, defense-in-depth arrangement of equipment, and other equipment diversity as outlined below (many of these features were included in the original protection system design; refer to Figure 7C-1 for details of how those additional diverse features, added as a result of the CMF analyses discussed in the previous section, have been implemented). Note that diverse equipment can be in the form of digital or non-digital devices as long as these devices are not subject to the same common mode failure as the primary protection system components:*

*(1) Protection system diversity*

*(a) Manual, hardwired, two-button scram*

*(b) Manual division trip via diverse, non-microprocessor logic*

*(c) Scram when reactor mode switch is placed in shutdown (hardwired)*

*(d) Manual MSIV closure (hardwired)*

*(e) ATWS mitigation [Alternate Rod Insertion (ARI) and FMCRD run-in, ADS inhibit, automatic Standby Liquid Control System initiation and feedwater runback] (hardwired and diverse digital system)*

*(2) Defense-in-depth configuration:*

*(a) Fail-safe RPS and fail-as-is ESF in separate processing channels*

*(b) Control systems are independent of RPS and ESF in separate triplicated processing network using diverse hardware and software from the Essential Multiplexing System network*

*(3) Equipment diversity*

*(a) Output logic units use discrete gate logic and provide trip seal-in and reset, division bypass, and manual trip functions*

*(b) The operator is provided with a set of diverse displays separate from those supplied through the safety-related, software-based logic. The displays listed below provide independent confirmation of the status of major process parameters:*

*(i) RPV water level*

*(ii) RPV water level 3 alarm*

*(iii) Drywell pressure*

*(iv) Drywell pressure high alarm*

*(v) CUW isolation valve status*

*(vi) RCIC steam line isolation valve status*

*(vii) HPCF flow*

*(c) Two containment isolation functions implemented with hardwired controls from the control room are also provided:*

*(i) CUW line inboard isolation valve manual initiation (for CUW LOCA outside the primary containment)*

*(ii) RCIC steam line inboard isolation valve manual initiation (for RCIC steam line break outside the primary containment)*

*(d) HPCF manual start in loop C (Division III) is implemented in equipment that is diverse from the automatic start function. All interconnections are hardwired and control and interlock logic is provided in the form of either discrete logic gates or programmable logic that is diverse from the automatic start logic. The signal path of the manual logic is independent from that of the automatic logic up to the actuated device drivers (e.g., motor control centers or switchgear). The manual start function is not implemented in the automatic logic; however, the logic reset switch is common to both the automatic and manual logic. In addition to the manual start function, which performs all necessary control actions as a substitute for automatic start, other supporting hardwired functions are provided in loop C as follows:*

*(i) Suction source selection*

*(ii) Manual open/close valve control of suppression pool suction valve F006*

*(iii) Manual open/close valve control of condensate storage pool suction valve F001*

*(iv) RPV level control*

*(1) Manual open/close valve control of injection valve F003*

*(2) Automatic minimum flow valve operation (F010)*

*(3) Hardwired thermal relay bypass logic*

*(4) Alarms and indicator lights for diverse logic status*

*(v) Remote shutdown system (analog, hardwired) provides shutdown cooling functions and continuous local display of monitored process parameters.*

*If the protection system is disabled because of common mode failure, the operator is expected to enter the emergency operating procedures at the appropriate points as determined by the indications on the hardwired backup displays and manipulate the control functions described above.*

*Additional diversity is available at the plant level even if SSLC is disabled because of common mode failure. The same common mode failure would not be expected to affect the feedwater control system, which, although not safety-related, is operated by a highly reliable, triplicated fault-tolerant control system that is diverse in both hardware and software from the safety systems. Similarly, makeup water is also available from CRD purge flow and condensate pumps. These additional sources of water will generally mitigate all Chapter 15 events, as discussed in the analyses described in section 7C.4 above; however, a channel of manually-initiated HPCF, as shown in item (4) above, has been added to meet worst-case conditions.* ]*

## 7C.6 References

(1) Chapter 19N, “Analysis of Common-Cause Failure of Multiplex Equipment”, ABWR Standard Safety Analysis Report, Amendment 33.

(2) J. Palomar, et al., “A Defense-in-Depth and Diversity Assessment of the GE ABWR Instrumentation and Control Systems, Version 3”, UCRL-ID-114000, Lawrence Livermore National Laboratory, April 30, 1993.

(3) Letter, David A. Ward to Ivan Selin, “Digital Instrumentation and Control System Reliability”, NRC, Sept. 16, 1992.

(4) Letter, James M. Taylor to David A. Ward, “Defense Against Common Mode Failures in Digital Instrumentation and Control (I&C) Systems”, NRC, Oct. 23, 1992.

(5) Letter, J. Fox to C. Poslusny, “Submittal Supporting Accelerated ABWR Review Schedule-I&C Diversity”, Docket No. STN 52-001, Feb. 26, 1993.

(6) Letter, J. Fox to C. Poslusny, “Submittal Supporting Accelerated ABWR Review Schedule-I&C Diversity Issue, DFSER Open Item 7.2.6-2”, Docket No. STN 52-001, June 18, 1993.

(7) Letter, J. Fox to C. Poslusny, “Submittal Supporting Accelerated ABWR Review Schedule-I&C Diversity (Issue #46)”, Docket No. STN 52-001, July 9, 1993.

* See Section 7A.1(1).

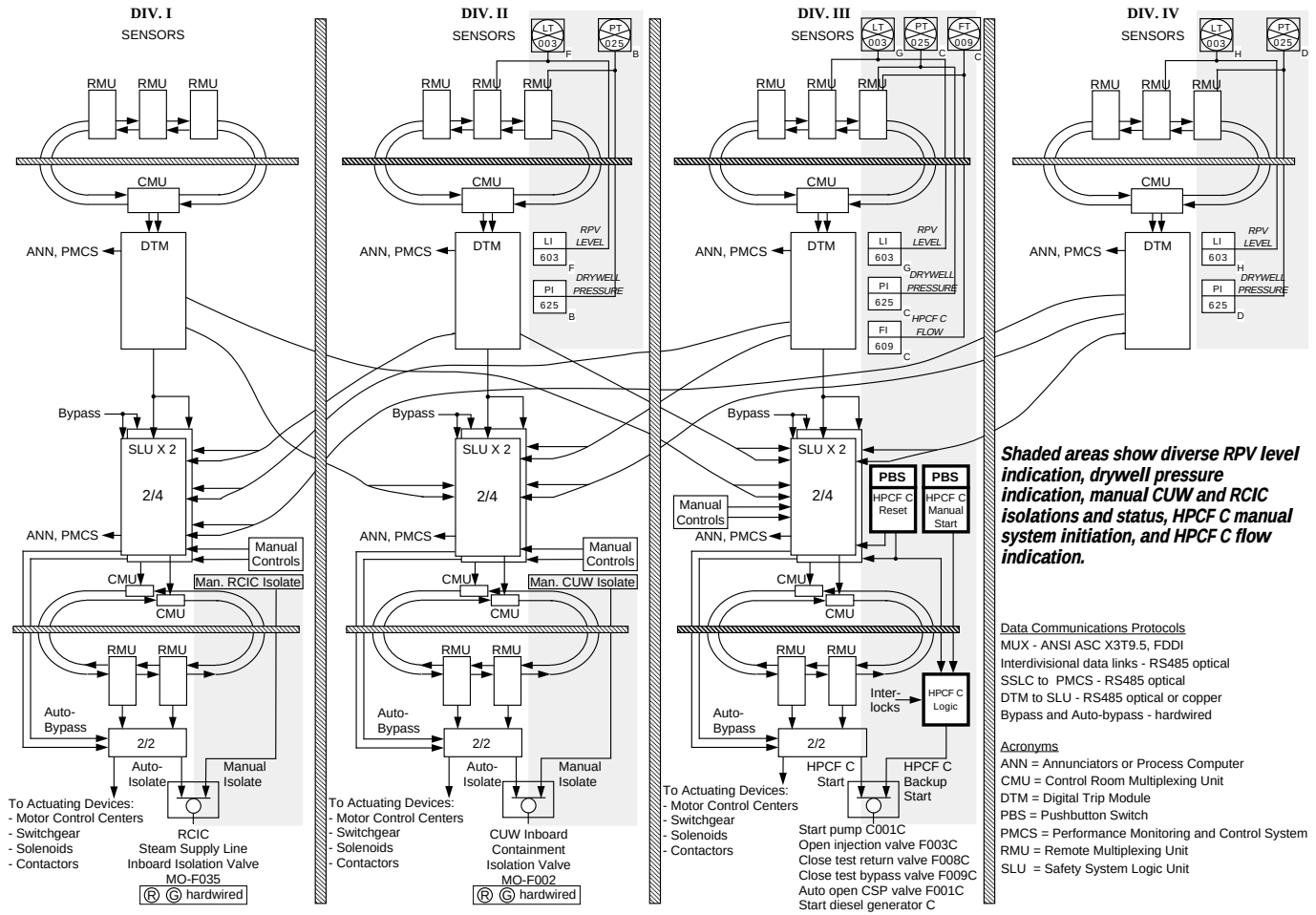



**Figure 7C-1 Implementation of Additional Diversity in SSLC to Mitigate Effects of Common-Mode Failures**