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

Refer to Section 7.9 for terminology related to the Reactor Trip and Isolation System (RTIS), the Neutron Monitoring System (NMS), and the Engineered Safety Features Logic and Control System (ELCS).

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 the safety system logic and control (SSLC). The SSLC includes multiple redundant divisions, which are separated from each other. The SSLC has four redundant divisions of sensors. Each division of sensors has a corresponding division that determines the trip status of the safety functions relative to the safety function setpoint. The SSLC has four redundant divisions for all actuation functions except for the engineered safety features. The engineered safety features have three divisions, corresponding to the maximum redundancy of the engineered safety features actuated components. Some engineered safety features functions are less than three-fold redundant and are assigned to the appropriate set of redundant divisions. 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.

Sensor signals are hardwired to the Reactor Trip and Isolation System. These sensors are divisionally separated.

Divisional separation is applied to the Essential Communication Functions (ECFs) of ELCS, which provides communication 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 include: (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 Temperature 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.

* See Section 3.5 of DCD/Introduction.

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.

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 reactor building essential electrical equipment rooms.

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. The Recirculation Flow Control System (upon detection of either high reactor dome pressure, low reactor water level or Manual ARI initiation) activates opening signals for the ARI valves of the Control Rod Drive (CRD) System (i.e., for backup hydraulic insertion of the control rods) and activates ARI initiation command signals to the Rod Control and Information System (i.e., for electric motor insertion of all operable control rods to the full-in position). This provides a method, diverse from the SCRAM function of the Reactor Protection System and associated CRD hydraulic control units (HCUs), for achieving insertion of control rods.

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)

The SRNM, LPRM, and APRM are the only safety-related subsystems of NMS.

7.1.1.6.2 Process Radiation Monitoring System (PRM) Instrumentation and Controls

The Process Radiation Monitoring System (PRM) 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. The only CAMS safety-related function is measuring radiation levels in primary containment.

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 determined in accordance with the instrument setpoint methodology document described in Subsection 16.5.5.2.11, Setpoint Control Program). 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 methods for calculatingsafety system setpoints are determined in accordance with the instrument setpoint methodology document described in Subsection 16.5.5.2.11, Setpoint Control Program, 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 RTIS and ELCS Systems can be tested during reactor operation. 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 test of the safety system logic and control which 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. With a division-of-sensors bypass in place, calibrated, variable signals are injected in place of the sensor signals and monitored for linearity, accuracy, fault response, and downscale and upscale trip response. 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 may 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 consists of an online, continuously operating, self-diagnostics and offline end-to-end surveillance program. Cross channel comparison of sensor inputs is performed by plant computer functions. Both online and offline functions operate independently within each of the four divisions. There are no multi-divisional interconnections associated with self-diagnostics.*

The primary purpose of the self-diagnostic function 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-diagnostic function eliminate the need for the other five manual tests. However, most faults are detected more quickly than with manual testing alone.

The self-diagnostic 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 ECF/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. Diagnostic testing is performed as part of the online functions during normal operation. Tests will verify the basic integrity of each card or module. All operations are part of normal data processing intervals and will not affect system response to incoming trip or initiation signals. Process or logic signals are not changed as a result of self-diagnostic functions.

The self-diagnostic function does not degrade system reliability. Indications of test results (pass, fail) is provided.

Self-diagnosis includes monitoring of overall program flow, and processor memory condition. Testing includes continuous error checking of all transmitted and received data; for example, error checking by parity check, checksum, or cyclic redundancy checking (CRC) techniques.

Actuation of the trip function is not performed during this test. The self-diagnostic 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-diagnostic failures (except intermittent failures) are annunciated to the operator at the main control room console and logged by the process plant *computer functions (PCFs). Faults are identified to the replacement board or module level and are generally indicated at the failed unit.*

The self-diagnostic function also includes power supply voltage levels and verification of the module configuration.

The Essential Communication Function (ECF) is included in the continuous, automatic self diagnostic function. Faults at the Remote Digital Logic Controllers (RDLCs) are alarmed in the main control room. ECF is dual in each division. A fault on one of the two communication paths will not prevent system operation through the unfaulted path.

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

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

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

Test failures are displayed on a front panel readout device or other diagnostic unit.

To reduce operator burden and decrease outage time, a maintenance and test panel (MTP) is provided as a dedicated instrument in each division of ELCS. The MTP is used for testing of ELCS 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) Interlock logic for each valve or pump.

A separate test sequence for each safety system is operator-selectable. Surveillance testing is performed in one division at a time. The surveillance test frequency is given in Chapter 16.

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.]*

* See Subsection 7.1.1.2.

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 Subsection 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 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 the ARI valves of the Control Rod Drive System or using the ARI motor run-in function of the Rod Control and Information System.

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

(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 (e.g., the stepping motor driver modules (SMDMs), which control the fine motion control rod drive (FMCRD) motors, shall derive their input power from a power bus that can automatically receive power from an emergency diesel generator, if necessary).

(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 separate instrumentation and controls in the main control room and 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 (Subsection 7.1.2.2).

(d) The SRNM subsystem will provide Anticipated Transient Without Scram (ATWS) permissive signals to the ESF Logic and Control System (ELCS).

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 x 10^3 neutron/cm^2 to 1.5 x 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.

The APRM subsystem also provides Anticipated Transient Without Scram (ATWS) permissive signals to the ESF Logic and Control System (ELCS) as described in Subsection 7.6.1.1.2.2(5).

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) Not Used

(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 the Offsite Dose Calculation Manual 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 continuously the radiation environment in the drywell and suppression chamber during reactor operation and under post-accident conditions. Monitoring shall be provided by two independent safety-related divisional subsystems of radiation monitors.

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.

Monitor the atmosphere in the inerted primary containment for concentration of hydrogen and oxygen gases, primarily during post-accident conditions. Monitoring shall be provided by two independent and redundant non-safety-related subsystems of Oxygen/Hydrogen Monitors.

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 loss of coolant accident (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.

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 Subsection 8.3.3.6.2)

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 603 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 603, Paragraph 5.8.3, Regulatory Guide 1.47, and BTP ICSB 21. Regulatory Guide 1.47 requires designs to satisfy Paragraph 4.13 of IEEE 279, which has been subsequently superceded by Paragraph 5.8.3 of IEEE 603. Bypass indications also satisfy these requirements. 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. Safety limits, setpoints, and margins are determined in accordance with the instrument setpoint methodology document described in Subsection 16.5.5.2.11, Setpoint Control Program.

* See Section 3.5 of DCD/Introduction.

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 IIEEE-603—Standard Criteria for Safety Systems for Nuclear Power Generating Stations

All safety-related systems are designed to meet the requirements of IEEE-603. Clarifications of any of the provisions are discussed for the applicable systems in the analysis portions of Sections 7.2, 7.3, 7.4, 7.6 and 7.9.

IEEE-603, Section 4, Safety System Designation

A specific basis is established to determine the design of each safety-related I&C system. This basis evolved from the identification of Design Basis Events (DBE) that are postulated in Chapter 15. The plant operating conditions and the safety analysis acceptance criteria applicable for each event are shown in Chapter 15. Credited systems, interlocks, and functions are evaluated for each DBE. Information provided for each design base item enables the detailed design of the system to be carried out. The number of sensors and their location, including spatial effects, is determined during this design basis analysis. The identification of variables are derived from the DBEs as well as the requirements for varied manual initiation and control of protective functions. Safety system design basis descriptions are included in the various sections of this Chapter.

IEEE-603, Sections 5, 6 and 7, Safety System Criteria

The safety-related systems are designed to maintain plant parameters within acceptable limits that are established by design basis events. This is done with precision and reliability meeting the requirements of IEEE-603. The scope of IEEE-603 includes safety-related I&C systems and is described in more detail in Sections 7.2 through 7.6 and 7.9. The safety-related I&C design conforms with IEEE-603 and has been qualified to demonstrate that all required performance requirements are met. Nonsafety-related systems generally are not required to meet any of the requirements of IEEE-603 with the exception of their independence from safety-related systems. The safety-related I&C design descriptions related to IEEE-603, Sections 5, 6, and 7 requirements are provided below.

(1) Paragraph 5.1, Single Failure: The safety-related I&C systems are designed to ensure that safety-related functions required for design basis events (DBE) are performed in the presence of: (a) single detectable failure within safety-related systems concurrent with all non-detectable failures; (b) failures caused by the single failure; and (c) failures and spurious system actions that cause, or are caused by the design basis event, requiring the safety-related functions as identified in the applicable failure modes and effects analysis (FMEA).

(2) Paragraphs 5.2 & 7.3, Completion of Protective Actions: The safety-related I&C systems are designed so that a) once initiated (automatically or manually), the intended sequence of the safety-related functions of the execution features continue until completion, and b) after completion, deliberate operator action is required to return the safety-related system to normal.

(3) Paragraph 5.3, Quality: A: safety-related I&C equipment is provided under the 10 CFR Part 50 Appendix B quality program. This satisfies all applicable requirements of the following: 1) 10 CFR Part 50 Appendix B and 2) ANSI/ASME NQA-1. The safety-related digital I&C software and/or firmware conform with the quality requirements of IEEE 7-4.3.2.

(4) Paragraph 5.4, Equipment Qualification: The safety-related I&C equipment is designed to meet its functional requirements over the range of environmental conditions for the area in which it is located. The equipment is designed to meet the equipment qualification requirements set forth by this criterion.

(5) Paragraph 5.5, System Integrity: The safety-related I&C systems are designed to demonstrate that the safety system performance is adequate to ensure completion of protective actions, over a range of transient and steady state conditions, as enumerated in the design basis.

(6) Paragraph 5.6, Independence: For the safety-related I&C systems, there is physical, electrical, and communication independence between redundant portions of safety-related systems and between safety-related systems and nonsafety-related systems, as discussed in the applicable Sections.

(7) Paragraph 5.7, Capability for Test & Calibration: The safety-related I&C systems are designed with the capability to have their equipment tested and calibrated while retaining their capability to accomplish their safety functions.

(8) Paragraph 5.8, Information Displays: The information display design is discussed in Chapter 18. This design process includes the necessary steps to ensure compliance with regulatory requirements and the guidance provided in RG 1.47 for bypass and inoperable status indication and in RG 1.97 for accident monitoring instrumentation as discussed in Section 7.5.

(9) Paragraph 5.9, Control of Access: The safety-related I&C systems have features that facilitate the administrative control of access to safety-related system equipment.

(10) Paragraph 5.10, Repair: The safety-related analog and digital based I&C systems are designed to allow the timely recognition of malfunctioning equipment location to allow the replacement, repair and/or adjustment. Self-diagnostic functions and periodic testing will identify and locate the failure. Individual bypassing allows the failed equipment to be replaced or repaired on-line without affecting the protection function.

(11) Paragraph 5.11, Identification: Safety-related I&C equipment conforms with the identification requirements of this criterion. Safety-related equipment is distinctly marked for each redundant portion of a system with identifying markings. Hardware components or equipment units have an identification label or a nameplate. For digital platforms, versions of computer hardware, software and/or firmware are distinctly identified. Proper configuration management plans are implemented as a way to formalize this identification process.

(12) Paragraph 5.12, Auxiliary Features: ABWR safety-related I&C system auxiliary supporting features satisfy the requirements of this criterion where applicable. For example, power supply and HVAC are key auxiliary supporting systems that satisfy the applicable requirements of IEEE-603. Other key auxiliary features are designed such that these components will not degrade the safety-related I&C systems below an acceptable level.

(13) Paragraph 5.13, Multi Unit Stations: Not applicable to single unit ABWR.

(14) Paragraph 5.14, Human Factors Considerations: Human factor scenarios are considered throughout all stages of the design process. Detailed information regarding these considerations can be found in Chapter 18.

(15) Paragraph 5.15, Reliability: The degree of redundancy, diversity, testability, and quality of the ABWR safety-related I&C design adequately addresses the functional reliability necessary to perform its safety protection functions. As stated above, the safety-related I&C equipment is provided under an Appendix B quality program.

(16) Paragraphs 6.1 and 7.1, Automatic Control: The safety-related I&C systems provide the means to automatically initiate and control the required safety-related functions.

(17) Paragraphs 6.2 and 7.2, Manual Control: The safety-related I&C systems have features in the main control room and remote shutdown system to manually initiate and control the automatically initiated safety-related functions at the division level.

(18) Paragraph 6.3, Interaction between the Sense and Command Features and Other Systems: The safety-related I&C systems meet the independence and separation requirements such that nonsafety-related systems failures will not affect of prevent any safety-related protection function. The normal communication path is one-way such that the safety-related systems will only broadcast to nonsafety-related systems and not vice versa. There is limited nonsafety-related communication under programmatic control to safety-related systems as discussed in Section 7.9.

(19) Paragraph 6.4, Derivation of System Inputs: To the extent feasible, the protection system inputs are derived from signals that directly measure the designated process variables.

(20) Paragraph 6.5, Capability for Testing and Calibration: The operational availability of the protection system sensors can be checked by perturbing the monitored variables, by cross-checking between redundant channels that have a known relationship with each other, and that have read-outs available, or introducing and varying substitute input to the sensor of the same nature as the measured variable. When one channel is placed into maintenance bypass mode, the condition is alarmed in the MCR and actuation logic capability is maintained to ensure the continued availability of all protective actions. Most sensors and actuators are designed to provide actual testing and calibration during power operation.

(21) Paragraphs 6.6 and 7.4, Operating Bypasses: The safety-related I&C systems automatically prevent the activation of an operating bypass whenever the applicable permissive conditions for an operating bypass are not met, and remove activated operating bypasses if the plant conditions change so that an activated operating bypass is no longer permissible.

(22) Paragraphs 6.7 and 7.5, Maintenance Bypasses: The capability of safety-related systems to perform their safety-related functions is retained when one division of the I&C systems is in maintenance bypass.

(23) Paragraph 6.8, Setpoints: Safety-related instrument setpoints are determined by a methodology that follows the guidance contained in Reference 7.3-2. This methodology ensures that characteristics such as range, accuracy, and resolution of the instruments meet the performance requirements assumed in the safety analyses in Chapter 15. The response times of the I&C systems are assumed in the safety analyses and verified by surveillance testing or system analyses.

The power source design requirements for the safety-related I&C systems are discussed in Chapter 8.

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.	Hardwired sensor interfaces.
	Nuclear system protection system (NSPS) solid-state-based logic and self-test system controllers.	Safety system logic & control (SSLC) configurable logic devices and microprocessor-based logic with self diagnostic functions.
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 Div. 2: LPCI + LPCI + ADS Div. 3: HPCS	Div 1: LPFL + RCIC + ADS Div II: HPCF + LPFL + ADS 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 (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.
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.

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

I & C System	GESSAR II Design	ABWR Design
	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.	This system deleted.
Standby Gas Treatment System:	Redundant active and passive components.	Redundant active components; two filter trains, two separate divisions.
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. Pump indication “RUN”, “STOP”, “TRIPPED”	Motor-operated-type injection valve. Pump indication “RUN”, “STOP”
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.

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

I & C System	GESSAR II Design	ABWR Design
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. 4 x 4 = 16 total T/Cs.	4 thermocouples in each of 4 divisions at 4 of 8 locations. 4 x 4 x 4 = 64 total T/Cs. 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)	**603**																						
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)	**603**																						
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)

	Regulatory Guide								BTP						II-D	II-E	II-F		II-K						
Applicable Criteria	**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)	**603**	**603**	**384**		**567.04**	**338**		**567.02**	**603**	**603**	**603**	**RG 1.47**	**RG 1.22**	**603**				**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												

Note: IEEE 603 has superceded the use of IEEE 279. In instances where NRC documents applicable to ABWR still refer to the outdated IEEE 279 standard, both the referenced IEEE 279 requirements and the analogous IEEE 603 requirements will be used. In cases of conflict between requirements in the different standards, IEEE 603 requirements govern.

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

	Regulatory Guide								BTP						II-D	II-E	II-F		II-K						
Applicable Criteria	**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)	**603**	**603**	**384**		**567.04**	**338**		**567.02**	**603**	**603**	**603**	**RG 1.47**	**RG 1.22**	**603**				**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																	

Note: IEEE 603 has superceded the use of IEEE 279. In instances where NRC documents applicable to ABWR still refer to the outdated IEEE 279 standard, both the referenced IEEE 279 requirements and the analogous IEEE 603 requirements will be used. In cases of conflict between requirements in the different standards, IEEE 603 requirements govern.

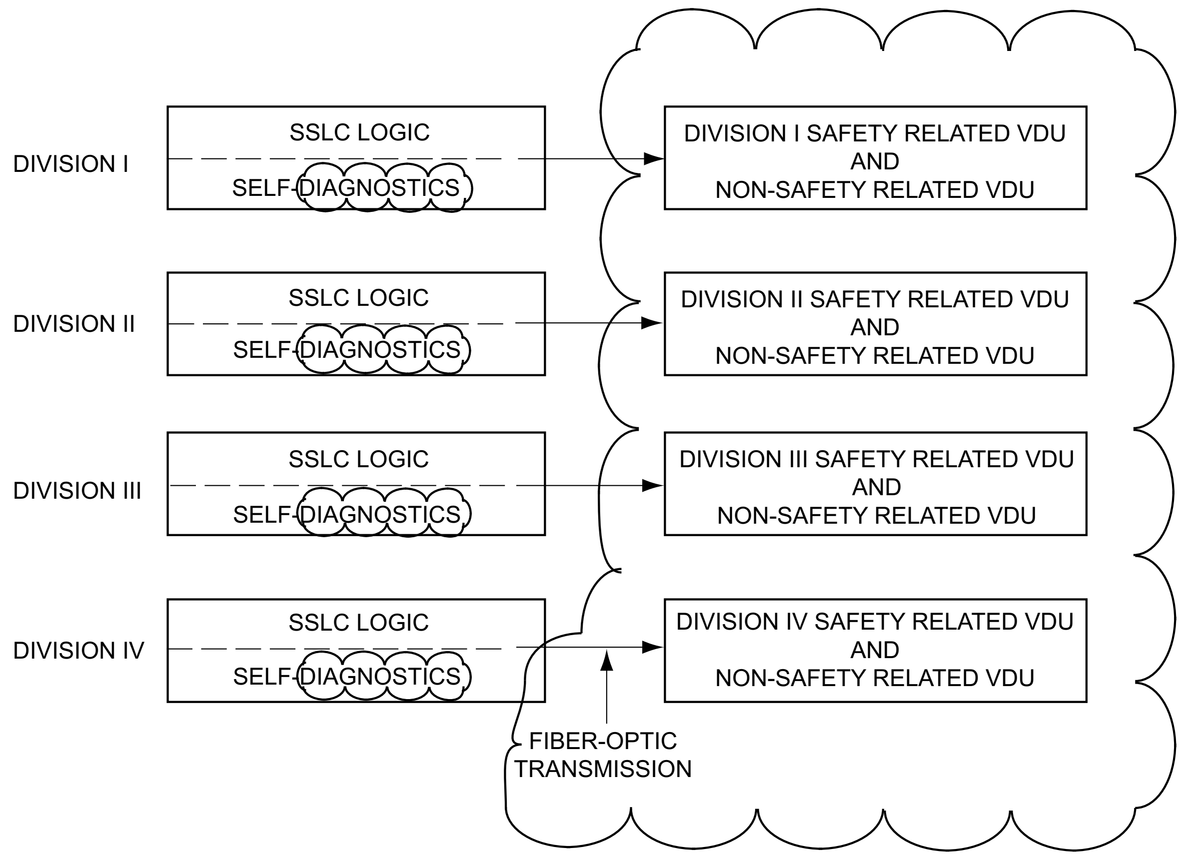
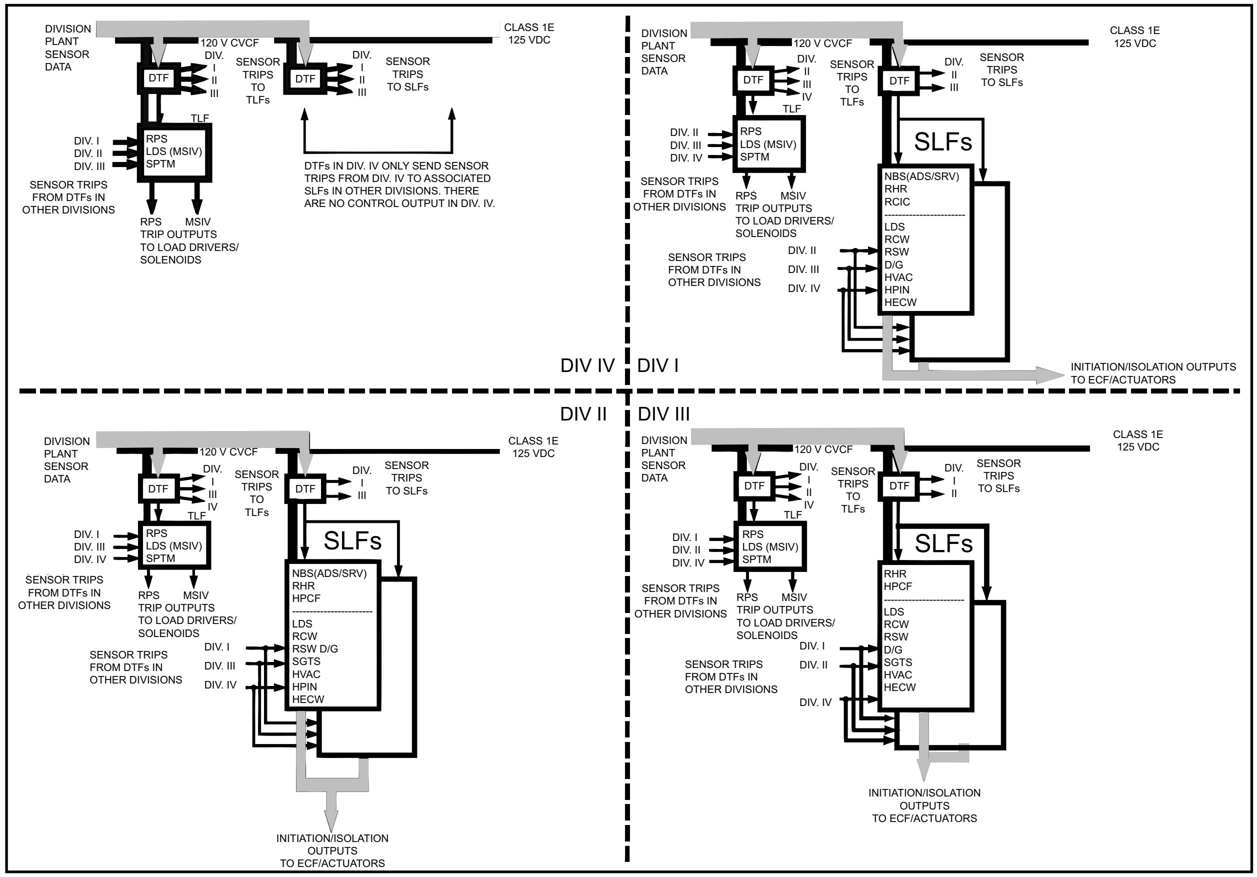


Figure 7.1-1 SSLC Self-Diagnosis



ABBREVIATIONS

DTF = DIGITAL TRIP FUNCTION
ECF = ESSENTIAL COMMUNICATION FUNCTION
SLF = SAFETY SYSTEM LOGIC FUNCTION
TLF = TRIP LOGIC FUNCTION

D/G = DIESEL GENERATOR
ESF = ENGINEERED SAFETY FEATURES
HECW = HVAC EMERGENCY COOLING WATER
HPCF = HIGH PRESSURE CORE FLOODER
HPIN = HIGH PRESSURE NITROGEN GAS SUPPLY
HVAC = HEATING, VENTILATING & AIR CONDITIONING
LDS = LEAK DETECTION & ISOLATION SYSTEM
MSIV = MAIN STEAM ISOLATION VALVE
NBS = NUCLEAR BOILER SYSTEM

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

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