

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 Standard Review Plan (SRP) NUREG-0800 (i.e., reactor trip system, engineered safety feature systems, safe shutdown systems, information systems important to safety, interlock system important to safety, control systems, diverse instrumentation and control systems, and data communication systems). Logic diagrams will be provided in the Final Safety Analysis Report (FSAR) for applicable I&C systems (see Table 7.1-3).

7.1.1.2 Safety System Logic and Control (SSLC)

7.1.1.2.1 Safety System Logic and Control (SSLC)

The integrated digital protection system, designated as safety system logic and control (SSLC), is the decision-making segment of RPS and ESF and provides their supporting structure (physical and functional). SSLC processes automatic and manual demands for reactor trip, ESF system initiation, or containment isolation based upon sensed plant process parameters or operator request. SSLC runs without interruption in all modes of plant operation to support the required safety functions.

The SSLC multi-divisional arrangement 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 safety-related instrumentation, and uses the input information to perform logic functions in making decisions for safety actions.

Most SSLC input data is multiplexed from process variables monitored by the essential multiplexing system (EMS) (refer to Section 7.9) in four physically and electrically isolated instrumentation divisions. Each of the four independent and separated EMS channels feeds an

independent and separated channel of SSLC equipment in the same division via remote multiplexing units (RMUs) that furnish plant sensor data to the fiber optic EMS network.

Signals without access to EMS, signals that must meet time response constraints, and signals from system logic that is in close proximity to the SSLC cabinets are directly connected to the four divisional cabinets in the main control room panel (MCRP) area. All signals to SSLC are derived from sensors that are redundant in the four divisions for each sensed variable. All input data, whether originally in analog form or discrete (contact closure) form, is converted and processed as serial-format digital bit streams within EMS and SSLC. RPS output signals in a division are sent to equipment actuators in that division by being hardwired directly as bistable trips. Alarm and status signals are sent from SSLC to the control room data network for computer logging and display. See Section 7.2 for a description of the performance of RPS.

The ESF output channels, which initiate slow-responding mechanical devices, are implemented via EMS. Control output signals in a division are sent to equipment actuators in that division by being multiplexed as digital messages to local Class 1E RMUs and then converted to bistable trips. A confirmed trip actuates a solid-state power switch, designated as a load driver (LD), at a Remote Multiplexing Unit (RMU) of EMS located in the control building (CB), reactor building (RB), or safety-related circulating water pumphouse. The trip is hardwired from the RMU to the equipment actuator (e.g., pump motor or motor-operated valve). ESF output channels reside only in Divisions I, II, and III because ESF mechanical equipment is in these three divisions and not in Division IV. See Section 7.3 for a description of the performance of each ESF system within SSLC.

SSLC does not require operator intervention during normal operation. However, abnormal conditions or maintenance activities require the operator to manually bypass a division of sensor inputs or a division of RPS trip logic. Since ESF trips are processed in dual-redundant channels of ESF outputs within a division, these trips are automatically bypassed and switched to the redundant backup channel on a sensed failure via self-test (manual output bypass is also available). Failure of automatic logic requires the appropriate emergency manual response (e.g., initiation of an emergency core cooling system or PCV isolation). However, all ESF loops have diverse or redundant backup loops in separate and independent mechanical and electrical divisions, so emergency manual initiation should not be required. Failure of automatic logic requires the appropriate emergency manual response (i.e., initiation of scram, containment isolation, or emergency core cooling system (ECCS) functions). Safety-critical automatic operations are provided with manual backup switches in each division for equipment initiation.

Manual control switches for reactor trip (scram) and main steamline isolation valve closure are independent of microprocessor-controlled logic. The two-button manual scram (and scram reset) of RPS is also independent of all logic that controls the LDs of the RPS scram pilot valve solenoids. Manual scram is performed by opening the power sources to the solenoids. Control switches for ECCS operate through dual-redundant microprocessor logic in each of the three ECCS divisions.

Testing and maintenance activities are supported through the use of manual control switches that activate the logic for the actuators of each safety system. In addition, self-diagnostic tests are performed continuously with SSLC on-line.

During normal plant operation, operator duties related to SSLC are restricted to correlating signal levels of the four divisions of redundant sensors by performing periodic visual cross-channel comparisons of the divisional MCRP displays of sensor signal levels.

Systems which utilize the SSLC include: (1) Reactor Protection 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 function of the Containment Monitoring System; and (7) Reactor Core Isolation Cooling System. Table 7.1-1 lists all safety-related systems and safety-related supporting functions supported by SSLC. The equipment arrangement for these systems and other supporting systems is shown in Figure 7.1-1. A detailed arrangement of RPS is shown in Figure 7.2-1.

7.1.1.2.1.1 SSLC Classification

SSLC components, as the supporting structure of RPS and ESF, are classified as Safety Class 2, Seismic Category I, and Quality Group B (electric Safety Class 1E) per Regulatory Guide 1.26 and meet the requirements of 10CFR50.55a(h).

7.1.1.2.1.2 Power Sources

To support the safety-related trip requirements of its interfacing systems, SSLC uses two types of power sources. Both sources are used simultaneously for redundant backup of the logic processors, which contain dual-redundant low voltage power supplies.

- (1) Class 1E 120 V vital AC (uninterruptible) is taken from the four divisional SSLC power supply buses discussed in Section 8.3. Each bus supplies power for one division of RPS logic equipment. 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 (see Section 7.2).
- (2) Class 1E 125 VDC—taken from the four divisional SSLC battery buses discussed in Section 8.3. Each of two divisional buses provide 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 (see Section 7.2). Each of the four divisional buses also provide power to a division of ESF logic equipment.

7.1.1.2.1.3 SSLC Equipment Design

- (1) Hardware Configuration

SSLC equipment resides in four independent and separated instrumentation divisions (I, II, III, and IV). SSLC integrates the control logic for the safety-related systems in each division into microprocessor-based, software-controlled, processing modules located in four divisional cabinets in the MCRP area (refer to Figure 7.1-1 for the assignment of system logic to SSLC processors).

Process sensors that directly initiate reactor trip or decay heat removal are replicated in the four divisions. Each division of SSLC logic performs functionally identical logical operations on the process sensor signals to initiate protective actions of the supported safety systems. Many sensor signals are shared by the control logic of multiple safety systems, thus significantly reducing the number of safety-related sensors in comparison to conventional plants. Shared sensors and shared logic can be implemented safely because 4-division, 2-out-of-4 coincident signal voting occurs simultaneously for the equivalent signals in the four divisions. This arrangement provides multiple independent trip channels that automatically accommodate random hardware and software failures.

The four redundant divisions provide a fault-tolerant architecture, as follows:

- (a) A division of equipment can be fully or partially bypassed for on-line maintenance, testing, and repair without losing reliable trip capability.
- (b) The system automatically defaults to 2-out-of-3 coincident voting in three operational divisions when a division of sensor inputs or trip logic is bypassed. This provides the safety systems with an extra measure of reliability and availability over alternative architectures, such as:
 - (i) Three-division, 2-out-of-3 voting, without bypass (typically used for the reactor control systems)
 - (ii) Two-division, 4-channel, 1-out-of-2 taken twice voting (typically used for protection system logic in conventional BWR plants)
- (c) The fault-tolerant arrangement conforms to safety system requirements for single failure tolerance, independence, and separation.

Additional discrete (non-microprocessor) logic is included to provide circuitry diverse from the microprocessors for trip seal-in and reset, logic channel bypass, manual scram, other manual control functions, and ATWS mitigation (see Section 7.8).

The four divisions are interconnected only by fiber optic communication links that are independent of EMS. These links transmit sensor trip data among the divisions for use in coincident logic that determines the final trip output status in each division. Fiber optic data links used as the transmission medium for interdivisional data have inherent properties of immunity to electrical noise (EMI, RFI, and lightning) and

provide point-to-point electrical isolation. Fiber optics are unaffected by the radiated noise from high voltage actuators, by high frequency motor control devices, and by transient switching pulses from electromagnetic conductors or other switching devices. The cable materials that protect and support the fibers are chosen to be flame retardant per the requirements of IEEE-323

Although logic processing for multiple systems is shared in the four divisions, several signal channels are provided within each division. This produces a segmentation of processing logic that decreases the probability of a common-mode failure of all processing channels.

Three Digital Trip Modules (DTMs) are provided in each SSLC division. One of the three DTMs is dedicated to monitoring the parameters associated with RPS trip and MSIV closure, both having a fail-safe response (i.e., loss of signal causes a trip). The input parameters to this DTM are process signals from sensors belonging to the following systems:

- (a) Main Steam (MS)
- (b) Leak Detection and Isolation (LDI)
- (c) Control Rod Drive (CRD)
- (d) RPS
- (e) Containment Monitoring System (CMS) [Suppression Pool Temperature Monitoring Function (SPTM) function]

Signals from the turbine building (TB) and MSIVs are hardwired to the DTM, since EMS is not available in these areas. Radiation sensor signals are processed within the divisional PRM cabinets in the MCR area, resulting in trip signals that are multiplexed on direct data links to the respective divisional DTMs within SSLC. The remaining signals are received via EMS.

The second and third DTMs contained in each SSLC division are dedicated to ESF. The parameters monitored for low pressure ECCS (RHR, ADS) and supporting ESF are received by one DTM, and the parameters monitored for high pressure ECCS (RCIC, HPCF) and supporting ESF are received by the other DTM. These parameters are process signals from the following systems:

- (a) Main Steam (MS)
- (b) Reactor Core Isolation Cooling (RCIC)
- (c) Leak Detection and Isolation (LDI)
- (d) Residual Heat Removal (RHR)

- (e) High Pressure Core Flooder (HPCF)
- (f) Reactor Building Cooling Water (RBCW)
- (g) Reactor Building Service Water (RBSW)
- (h) Reactor Water Cleanup (RWCU)
- (i) Condensate Storage and Transfer (CST)
- (j) Atmospheric Control System (ACS)

Separate voting and interlock logic channels are provided for the fail-safe (de-energize-to-trip) plant protection functions (RPS trip and MSIV closure) in Trip Logic Units (TLUs) and for the fail-as-is (energize-to-operate) functions (ECCS and supporting ESF) in Safety System Logic Units (SLUs). The SLU logic channels are dual-redundant in each division to prevent inadvertent ECCS/ESF initiation. The logic channels perform coincident signal comparisons and generate a final trip signal based upon interlock permissive and operator requests (manual control switches).

The RPS and MSIV output channels are hardware-based and hardwired. These channels perform final trip seal-in and implement the divisional bypass features. The ECCS/ESF output channels are implemented via EMS. These channels confirm the final trip state by performing a 2-out-of-2 comparison on signals from the redundant SLU channels at the output RMUs of EMS. A confirmed trip actuates LDs that are hardwired to safety system device actuators.

(2) Software Development

Software for SSLC operation is developed or purchased and qualified for safety-related use together with the microprocessor-based controller hardware according to the software management plans described herein. Software-based control programs are embedded as firmware [i.e., programmed into programmable read-only memory (PROM)] in the controller hardware and cannot be changed during operation.

This section defines the requirements to be met by the hardware and software development implementation activities for safety-related systems supported by SSLC. A Software Management Plan, Configuration Management Plan, and Verification and Validation Plan shall be generated to meet the following requirements (these plans conform to the guidance of BTP- HICB-14):

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 NQA2a, Part 2.7, Quality Assurance Requirements of Computer Software for Nuclear Facility Application
 - (iii) ANSI/IEEE-ANS-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, 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;
 - (ix) IEEE 1074, Standard for Developing Software Life Cycle Processes
- (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 into the software design the safety-critical software functions specified in the software requirements specification
 - (iv) identify in the coding and testing 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.

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, 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.
- (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.

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 829, Standard for Software Test Documentation Plans
 - (ii) IEEE 1008, Standard for Software Unit Testing
 - (iii) IEEE 1012, Standard for Software Verification and Validation Plans
 - (iv) IEEE 1028, Standard for Software Reviews and Audits
 - (v) ANSI/IEEE-ANS-7-4.3.2, Standard Criteria for Digital Computers Used in Safety Systems of Nuclear Power Generation Stations
 - (vi) IEC 880, Software for computers in the safety systems of nuclear power stations.
- (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 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.
- (3) Data Communications

Communication protocols used for data transmission (1) between SSLC controllers, (2) between redundant divisions of SSLC, (3) to and from the multiplexing network, and (4) for transferring data to the non-safety-related systems conform to ISO 7498, "Open Systems Interconnection- Basic Reference Model." At the Data Link Layer defined by ISO 7498, the protocols necessary to move data to the higher levels of the ISO model are defined in IEEE-802.2, "Standard for Local Area Networks: Logical Link Control." At the Physical Layer and Data Link Layer, data communications for point-to-point data transfer are implemented using RS-485 at a minimum data rate of 10 Mbits/sec over fiber optic cable.

Data communication is asynchronous among the redundant logic channels in the four divisions of SSLC equipment (i.e., there is no master clock and the clocks of the transmitting and receiving controllers are not synchronized by exchanging timing data). In addition, although acquired data is time tagged with a common time of day for convenience in logging and recording, the time tag is not required or used for safety-related functions. These practices ensure independent channel operation and no degradation of other divisions if one SSLC division completely or partially fails.

7.1.1.2.1.4 Main Control Room Area

Virtually all logic processing hardware within the RPS and ESF design scope is located within the four separate and redundant safety system logic and control (SSLC) cabinets in the main control room area. The RPS scram pilot valve fuse panels and the equipment for initiating RPS

scram time testing are located outside the main control room area. The SSLC panels are mounted in the divisional back panel areas of the main control room. The major system control switches, including bypass switches, are located on the main control console.

7.1.1.2.1.5 Control Room Cabinets and Their Contents

The SSLC logic cabinets, which contain the RPS and ESF functions for Divisions I, II, III, and IV, include a separate cabinet for each division. The cabinets contain digital and solid-state discrete and integrated circuits used to condition signals transferred to the SSLC from 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. Most logic functions are implemented in software permanently embedded in digital memory. However, some functions remain hardwired for reasons of diversity or speed of response. Load drivers with solid-state switching outputs for actuation of solenoids, motor control centers, or switchgear are located in the control room area in a separate bay of the SSLC cabinets.

The following major components implementing the above functions are located in each SSLC cabinet:

(1) Digital Trip Module

Performs sensor channel trip decisions (comparison of input variables to programmed setpoints) and sends these decisions to four divisions of Trip Logic Units.

(2) Trip Logic Unit (for RPS) or Safety System Logic Unit (for ESF)

(a) Performs system coincidence trip decisions (any two or more divisions of instrumentation must simultaneously provide a tripped sensor channel output from a DTM to ensure a tripped condition in any division for any set of four redundant sensors).

(b) Provides interlock logic permissives (e.g., from valve position switches or limit switches) that implement system functional logic as defined on the logic diagrams of the affected safety systems.

(c) Transmits outputs to operator displays and the plant computer system via digital data links or the control room data network, including annunciator outputs from built-in self-diagnostic functions

(3) Output Logic Unit (RPS and MSIV)

Provides sealed-in trip logic outputs from SSLC to the actuated devices that initiate the appropriate plant protection equipment (e.g., scram pilot valve or MSIV pilot

valve solenoids) and also provides divisional trip logic bypass capability. This unit is implemented with discrete, hardware-based logic to be diverse from the software-based controllers that it bypasses.

(4) Suppression Pool Calculation Module

Provides bulk average suppression pool temperature from an input array of temperature sensors located in four quadrants of suppression pool. Output signals are processed in the RPS DTM as a reactor trip variable and in the ESF1 DTM (see Section 7.3) as an initiation signal for RHR suppression pool cooling and RBCW load shedding.

(5) Load Drivers

Load drivers are trip actuators that implement RPS output coincidence logic by means of their arrangement and interconnections. The load drivers (LDs) are bistable, solid-state, 120 VAC current-interrupting devices that are normally kept energized to maintain the fail-safe structure of the trip systems. A trip signal on the input side of the LDs (which is sent from the OLU) creates a high impedance, current-interrupting condition on the output side. The LDs are inserted in the power circuit path between the scram pilot valve solenoids and their power source such that when in the tripped state, they cause de-energization of the scram pilot valve solenoids. The LDs are components of SSLC and are located in the SSLC divisional cabinets in the MCR back panel area. The main control console contains the reactor mode switch, the RPS manual scram pushbutton switches, the CRD scram reset switches and the bypass switches for the low CRD HCU accumulator charging pressure. The wide display behind the main control console contains SSLC bypass switches that can bypass process sensor inputs to each RPS channel's trip logic and can also bypass divisional trip logic outputs to the actuating devices for the scram pilot valve solenoids.

7.1.1.3 Reactor Trip System

7.1.1.3.1 Reactor Protection System (RPS)

The Reactor Protection System (RPS) 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 and limits system pressure, thereby restricting the release of radioactive material.

7.1.1.4 Engineered Safety Features (ESF) Systems

7.1.1.4.1 Emergency Core Cooling Systems (ECCS)

Instrumentation and controls provide automatic initiation and control of specific core cooling systems such as High Pressure Core Flooder System (HPCF), Automatic Depressurization

System (ADS), Reactor Core Isolation Cooling System (RCIC) and the low pressure flooders mode of the Residual Heat Removal System (RHR) provided to cool the core fuel cladding following a design basis accident.

7.1.1.4.2 Leak Detection and Isolation System (LDI)

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.

7.1.1.4.3 RHR Wetwell and Drywell Spray (WDCS) Mode

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.

7.1.1.4.4 RHR Suppression Pool Cooling (SPC) Mode

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

7.1.1.4.5 Standby Gas Treatment System (SGT)

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

7.1.1.4.6 Emergency Diesel Generator (EDG) Support Systems

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

7.1.1.4.7 Reactor Building Cooling Water and Reactor Building Service Water Systems (RBCW and RBSW)

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

7.1.1.4.8 Essential HVAC Systems (HVAC)

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

7.1.1.4.9 Emergency Chilled Water System (ECW)

Automatic instrumentation and control is provided to assure that adequate cooling is provided for the Control Room Habitability Area (CRHA), the control building safety-related electrical equipment (CBSREE) rooms, and the Reactor Building safety-related equipment area (RBSREA) cooling coils.

7.1.1.4.10 Nitrogen Supply System (N₂)

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

7.1.1.4.11 Flammability Control System (FCS)

The LOCA signal from the MCR is used as the preliminary initiation signal for FCS operation. However, the actual initiation and operation of the primary FCS recombiner unit is based on the increases in the hydrogen and oxygen concentrations within the PCV as measured by the Containment Monitoring System (CMS) during the analysis of the LOCA. FCS is manually initiated by the operator.

7.1.1.5 Safe Shutdown Systems

7.1.1.5.1 Residual Heat Removal (RHR) System/Shutdown Cooling Mode

Instrumentation and controls provide information and capabilities for manual alignment of cooling systems to remove the decay and sensible heat from the reactor vessel.

7.1.1.5.2 Remote Shutdown System (RSD)

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

7.1.1.5.3 Standby Liquid Control System (SLC)

Instrumentation and controls are provided for the manual initiation of an independent backup system, (i.e., the SLC). The SLC 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 fine motion control rod drives (FMCRD) fail to shut down the reactor during an anticipated transient without scram (ATWS) event as described in Subsection 7.8, then instrumentation and controls are provided for the automatic initiation of SLC.

7.1.1.6 Information Systems Important to Safety

7.1.1.6.1 Post Accident Monitoring (PAM)

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.

7.1.1.6.2 Process Radiation Monitoring System (PRM) Instrumentation and Controls

The PRM 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 provides the Plant Computer System (PCS) with alarm of high radiation levels. In turn, the PCS will transmit this information to the main control room (MCR) to alert operating personnel to the high radiation activity.

7.1.1.6.3 Containment Monitoring System (CMS)

The containment atmospheric monitoring function of CMS provides normal plant operation and post-accident monitoring for gross gamma radiation and hydrogen/oxygen concentration levels in both the drywell and wetwell. CMS also continuously monitors suppression pool temperatures during reactor operation for automatic reactor scram or suppression pool cooling initiation. Drywell pressure is also continuously measured to provide actuation signals to LDI. The Lower Drywell Flooding (LDF) function of CMS can be used to flood the lower drywell with water from the suppression pool in the unlikely event of a severe accident.

MCR display and annunciation indicate the gamma, hydrogen/oxygen levels, suppression pool temperature and drywell pressure under all operating and accident conditions.

7.1.1.7 Interlock System Important to Safety

7.1.1.7.1 RHR High Pressure/Low Pressure Systems Interlock Function

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

7.1.1.7.2 Wetwell-to-Drywell Vacuum Breaker Interlocks

This system is provided to automatically prevent the occurrence of undesirable negative pressure differential on the containment shell liner (see Subsection 6.2.1).

7.1.1.8 Control Systems

Control Systems are not safety related except for major portions of the Neutron Monitoring System (NMS), which are discussed below.

7.1.1.8.1 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 RPS to automatically shut down the reactor when a condition necessitating a reactor scram is detected. The NMS is composed of the following subsystems, which are classified as indicated.

- (1) Startup Range Neutron Monitor (SRNM) (Safety-Related)
- (2) Local Power Range Monitor (LPRM) (Safety-Related)
- (3) Average Power Range Monitor (APRM) (Safety-Related)
- (4) Oscillation Power Range Monitor (OPRM) (Safety-Related)
- (5) Automated Traversing Incore Probe (ATIP) (Non-Safety-Related)
- (6) Multi-channel Rod Block Monitor (MRBM) (Non-Safety-Related)

7.1.1.9 Diverse Instrumentation and Control Systems

Although not required for safety, diverse I&C is provided for ATWS mitigation including alternate control rod insertion, and manual hard-wire start capability for selected protection systems.

7.1.1.10 Data Communication Systems

7.1.1.10.1 Multiplexing System

The MUX provides distributed control and instrumentation data communications networks to support the monitoring and control of interfacing plant safety and non-safety systems. It provides all the electrical devices and circuitry (such as multiplexing units, data transmission line and transmission controllers) between sensors, display devices, controllers and actuators. MUX utilizes acquisition and communication software required to support its function of transmitting plant-wide data for distribution control and monitoring.

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) NRC Regulatory Guides
- (3) NRC Branch Technical Positions
- (4) Industry codes and standards

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 and margins are provided in Chapter 16 of the FSAR). 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.

7.1.2.1.5 Technical Design Bases

The technical design bases for the instrumentation and control systems are provided in Subsection 7.1.2.2 through 7.1.2.9. The design bases in Subsections 7.1.2.2 and 7.1.2.3 are also applicable to the SSLC as the supporting physical and functional structure of RPS and ESF Systems.

7.1.2.1.6 SSLC Inservice Testability

(1) Surveillance Testing

Extensive built-in self-testing is implemented in the digital SSLC design to support RPS and ESF operation and to improve availability by decreasing downtime.

Most SSLC surveillance testing is included as part of surveillance testing for its supported safety systems, since SSLC contains the control logic for these systems. For example, placing an RHR loop in test mode requires the SSLC logic channel and output channel for that loop to evaluate the request and send signals to the device actuators that perform the requested action. For information on tests that are not part of SSLC, refer to the following:

- (a) Manual scram testing is described in Section 7.2.
- (b) NMS calibration is described in Subsection 7.7.1.6.
- (c) Single rod scram test is described in Section 7.2 and Subsection 7.7.1.2.
- (d) Calibration of analog sensor inputs is described in Subsection 7.1.2.1.6.
- (e) The sensor check is described in Section 7.2.
- (f) The integrated self-test is described in Subsection 7.1.2.1.6.

However, the following surveillance tests are unique to SSLC, since they involve functions shared by all interfacing systems:

- (a) **Sensor Channel Check** - Performance of this check provides confidence that a gross failure of a device in a sensor channel has not occurred. This check is a visual comparison, on the MCR main control console, of the parameter indicated in one sensor channel to a similar parameter in a different sensor channel. Since redundant sets of sensors measure the same process, the indications should be reasonably close. This check is performed every shift.
- (b) **Divisional Functional Test** - A divisional functional test or channel functional test provides confidence that the software-based control programs within the

SSLC controllers perform as intended. The test is performed by replacing the process signal with a test signal generated by the SSLC Surveillance Test Controller. The test signal, which can simulate the full range of an analog or digital process signal, is injected at the RMU input of EMS to test the DTMs. The as-found trip setpoints are confirmed to be within their allowable values. Test signals are also injected at the TLUs (see Section 7.2) and safety system logic units (SLUs) (see Section 7.3) to check trip logic and interlock logic response. The DTMs, TLUs, and SLUs contain test input and output jacks to accommodate test equipment connections. Switches are provided to connect and disconnect inputs and ports from the test condition. Test status is displayed in the main control room. The Test Controller monitors, evaluates, and logs the tested channel outputs. The Test Controller automatically cycles through tests for all sensor inputs of all safety systems within SSLC. However, the 2-out-of-4 logic is not tested, since inputs from multiple divisions would be required. When the tests are completed, the Test Controller removes all input signals and verifies that trip outputs are cleared. Trip signal status is indicated at the Test Controller. This test is performed on-line with a sensor channel or logic channel bypassed, so that spurious trips are prevented. The Test Controller is not connected during normal SSLC operation. This test, performed quarterly, supplements the continuous self-diagnostic checks within each SSLC controller.

- (c) **Comprehensive Functional Test**- This test, which is performed during an outage, verifies overall SSLC system function, computer component function, software and hardware interactions, response times, and error handling in four divisions. Error statistics, usage statistics, historical statistics, and various other measures are used to verify proper performance of SSLC. Successful completion of these tests establishes operability of sensor channels, logic channels, and output channels. This end-to-end test injects test signals simultaneously in the four divisions at the RMU inputs and thus checks the 2-out-of-4 voting logic. The software-based SSLC contains many states, not all of which will occur over the life of the plant. The most important states are those that are required to mitigate accidents. Therefore, this test focuses on usage testing, which exercises the overall system by simulating the input conditions under which the system is designed to perform, rather than coverage testing, which attempts to exercise all possible states of the system. This test assures that the protective action equipment is within its specified performance characteristics.
- (d) **Sensor Channel Calibration** - A sensor channel calibration or channel calibration is a complete check of the instrument loop and the sensor. This test verifies that a channel responds to the measured parameter within the necessary range and accuracy. Calibration leaves the channel adjusted to

account for instrument drift between successive calibrations. The calibration includes all parameters used to establish derived setpoints (e.g., Thermal Power Monitor setpoint) and all parameters used to automatically bypass a trip function (e.g., <40% Reactor Thermal Power bypass of Turbine Stop Valve closure). This calibration, performed during outages, supplements the automatic calibration features of SSLC and EMS, which adjust the analog-to-digital (A/D) converters under software control.

This calibration includes calibration of the analog trip modules (ATMs) used to implement the ATWS mitigation features (see Section 7.8).

(2) SSLC Controller Testing

The operating system of each microprocessor-based controller runs a self-test diagnostic program as the lowest priority background task, performing internal diagnostic functions and providing error messages and alarm outputs to the MCR displays. The self-test provision consists of on-line, continuously-operating self-diagnostics and an off-line semi-automatic (i.e., operator-initiated, but automatic-to-completion) test program, as described below. The off-line test includes trip testing of controller trip and initiation functions and is performed with a channel bypassed. Both on-line and off-line functions operate independently within each of the four SSLC divisions.

A hierarchy of test capability is provided to ensure maximum coverage of all SSLC functions, including both functional logic and communication links. Testing, which conforms to the requirements of Reg Guide 1.22, the associated guidance in BTP-HICB-8, and Reg Guide 1.118, includes:

(a) On-line Continuous Testing of SSLC Controllers

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

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 controlled for example, error checking by parity check, checksum, or 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 and load drivers are not tested. The self-test function is capable of detecting and logging intermittent failures without stopping system operation. Normal surveillance by plant personnel identifies these failures, via a diagnostic display, for preventive maintenance.

Self-test failures (except intermittent failures) are annunciated to the operator at the MCR console and logged by the plant computer system. Faults are identified to the replacement board or module level and positively indicated at the failed unit.

Continuous monitoring also includes power supply voltage levels and card-out-of-file interlocks. Out-of-tolerance conditions result in an inoperative (out-of-service) condition for that particular system function.

(b) Off-Line Semi-Automatic Testing of SSLC Controllers

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

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

Self-test failures are displayed locally at the SSLC controller and on the main control console.

(c) Off-line End-to-End System Testing (including EMS)

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 on each system logic diagram:

- (i) Each 2-out-of-4 coincident logic function
- (ii) Serial and parallel I/O, including manual control switches, limit switches, and other contact closures
- (iii) The trip calculation logic, including the interlock logic for each valve or pump

A separate test sequence for each safety system is operator-selectable. Testing proceeds automatically to conclusion after initiation by the operator. Testing is performed in one division at a time.

The STC injects test patterns through the EMS communication links to the RMUs. It then tests the RMUs' ability to format and transmit sensor data through the EMS/SSLC interface, in the prescribed time, to the LDs.

All test features adhere to the single-failure criterion, as follows:

- (i) No single failure in the test circuitry shall incapacitate an SSLC safety function.
- (ii) No single failure in the test circuitry shall cause an inadvertent scram, MSIV closure, other PCV isolation, or actuation of any ECCS/ESF system.

Watchdog timers are included in each SSLC controller to ensure that the microprocessor is operating properly. The timer reset is designed such that the software cannot enter an infinite loop and reset the timer as part of the loop sequence.

Self-test software is designed to detect potentially unsafe conditions and states and recovers to a safe state, while alerting the operator to the anomaly detected, the action taken, and the new, safe-state system configuration. All detected system errors are logged in controller memory and the plant computer system.

7.1.2.1.7 Environmental Considerations

Electrical equipment for SSLC is located in the Control Building. The environmental conditions for this area are shown in Section 3.11.

Control of the electromagnetic environment is also important in preventing degraded operation of sensitive, software-based, control equipment. Electromagnetic compatibility of the logic processors in SSLC is assured by conformance to the following program:

- (1) SSLC components are designed to minimize both susceptibility to, and generation of, EMI and RFI. Component design follows the guidance contained in IEEE Std. 518, Guide for the Installation of Electrical Equipment to Minimize Electrical Noise Inputs to Controllers from External Sources
- (2) EPRI TR-102323, "Guidelines for Electromagnetic Interference Testing in Power Plants," shall be used as test guidance in development of SSLC electronic equipment. The test results shall demonstrate that the susceptibility level of the tested digital

equipment shall be at least 8 db higher than the recommended allowable plant level and the emission level of the tested equipment shall be at least 20 db lower than the susceptibility level.

- (3) In applying EPRI TR-102323, the following basic standards will be employed as recommended in the guideline:
 - (a) 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.”.
 - (b) Equipment shall also comply with standard surge withstand capability tests, as follows:
 - (i) ANSI/IEEE-C62.41—Guide for Surge Voltages in Low-Voltage AC Power Circuits.
 - (ii) 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.

- (4) For design guidance and additional test development guidance, the following military standards shall be used:
 - (a) MIL-STD-461D—Electromagnetic Emission and Susceptibility Requirements for the Control of Electromagnetic Interference.
 - (b) MIL-STD-462D—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 U. S 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.

- (5) 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 Equipment to Minimize Electrical Noise Inputs to Controllers from External Sources
 - (b) IEEE Std. 1050, Guide for Instrumentation and Control Equipment Grounding in Generating Stations.

7.1.2.2 Reactor Protection 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 System (RPS) and its supporting instrumentation and control system apparatus, Safety System Logic and Control (SSLC) 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/SSLC 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/SSLC 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) No single failure within the RPS/SSLC shall prevent proper RPS action when required to satisfy Safety Design Bases as described by a, b, and c above.
- (l) 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.
- (m) 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/SSLC operational reliability and precision will be degraded by operator error:

- (n) Access to trip settings, component calibration controls, test points, and other terminal points shall be under the control of plant operations supervisory personnel.
- (o) Manual bypass of instrumentation and control equipment components shall be under the control of the MCR operator. If the ability to trip some essential part of the system has been bypassed, this fact shall be continuously annunciated in the MCR.
- (p) 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.
- (q) Provides manual control switches for initiation of reactor scram by plant operator when necessary.
- (r) 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 instrumentation and control portion of RPS (i.e., SSLC) are shown in Table 7.1-2.

(2) Non-Safety-Related Design Bases

The RPS/SSLC 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 instrumentation and controls portion of ECCS (i.e., SSLC) shall be designed to meet the following requirements:

- (a) Automatically initiate and control the Emergency Core Cooling System (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 MCR instrumentation.
 - (iii) Provision for manual control of the ECCS in the MCR.

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 (LDI)—Instrumentation and Controls

(1) Safety Design Bases

The general functional requirements of the Leak Detection and Isolation System (LDI) 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, LDI shall be designed 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 LDI 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 LDI 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 and initiation of isolation functions.

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 shall provide instrumentation and controls within SSLC 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) Provide information (from wetwell and drywell pressure sensors) to the operator for 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 from the MCR.
- (d) Indicate performance of the wetwell and drywell spray from the MCR.

Specific Regulatory Requirements:

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

- (2) Non-Safety-Related Design 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.

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 (SGT)—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 (EDG)—Instrumentation and Controls

- (1) Safety Design Bases

General Functional Requirements:

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

Specific Regulatory Requirements:

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

- (2) Non-Safety-Related Design Bases

There is no power generation non-safety-related design basis for this system.

7.1.2.3.7 Reactor Building Cooling Water and Service Water Systems (RBCW and RBSW)—Instrumentation and Controls

- (1) Safety Design Bases

General Functional Requirements:

The general functional requirements of the instrumentation and controls of these systems shall be to:

- (a) Maintain control of cooling water to equipment that requires cooling during reactor shutdown modes and following a LOCA or LOOP or both.
- (b) Provide for the automatic isolation of the non-essential parts of the Reactor Building Cooling Water System (RBCW) from the essential parts during a LOCA or upon detection of a major RBCW leak in the non-essential portion.
- (c) Provide for the automatic isolation of all parts of the Reactor Building Service Water (RBSW) Division outside of the Control Building upon receipt of a high water level signal in the RBCW Heat Exchanger Room in that division.

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 RBCW and RBSW shall be capable of being tested during normal plant operation.

7.1.2.3.8 Essential HVAC Systems (HVAC)—Instrumentation and Controls

- (1) Safety Design Bases

See Subsections 9.4.1 (Control Building HVAC), 9.4.5 (Reactor Building HVAC) and 9.4.15 (Auxiliary Fuel Building HVAC).

7.1.2.3.9 Emergency Chilled Water System (ECW)—Instrumentation and Controls

- (1) Safety Design Bases

General Functional Requirements:

The general functional requirements of the Emergency Chilled Water System (ECW) 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 offsite power, or isolation of normal heating, venting, and air conditioning (HVAC). During detailed design, a site-specific MCR temperature rise analysis shall be performed for the Station Blackout (SBO) scenario.

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 Nitrogen Supply System (N₂)—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 (SRVs) 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 non-safety-related design basis for this system.

7.1.2.3.11 Flammability Control System (FCS)

(1) Safety Design Bases

General Functional Requirements:

The safety-related components of FCS inside the Reactor Building are protected from postulated missiles and pipe whip, as required to assure proper functional integrity. FCS has the ability to withstand the dynamic effects associated with a safe shutdown earthquake (SSE) without loss of isolation function. FCS is designed so that all components exposed to the PCV atmosphere are capable of performing their safety-related function under the temperature, humidity, pressure, and radiation transients associated with a design basis LOCA. The FCS equipment valves and

instrumentation and controls are designed to withstand the thermodynamic and radiological environmental conditions inside the Reactor Building secondary containment during a design basis LOCA. FCS is capable of being functional tested to verify the ability of the system to perform its safety function.

Specific Regulatory Requirements:

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

(2) Non-Safety-Related Design Basis

There are no specific non-safety-related design basis for this system.

7.1.2.4 Safe Shutdown Systems—Instrumentation and Controls

7.1.2.4.1 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 controls as required to:

- (a) Enable the system to remove the residual heat (decay heat and sensible heat) from the reactor vessel during emergency shutdown when the vessel pressure is below approximately 931 kPaG.
- (b) Provide manual controls for the shutdown cooling system in the MCR and at the RSD panel.
- (c) Indicate performance of the shutdown cooling system by MCR instrumentation and controls in the RSD 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 and controls to enable the RHR to accomplish the following:

- (a) Provide cooling for the reactor during normal shutdown operation when the vessel pressure is below approximately 931 kPaG in preparation for refueling.

- (b) Cool and maintain reactor water at a temperature which is practical for refueling and servicing operation.

7.1.2.4.2 Remote Shutdown System (RSD)—Instrumentation and Controls

- (1) Safety Design Bases

General Functional Requirements:

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

- (a) Instrumentation and controls outside the MCR 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.
- (c) Protective functions in the event the MCR becomes uninhabitable.

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.

7.1.2.4.3 Standby Liquid Control System (SLC)—Instrumentation and Controls

- (1) Safety Design Bases

General Functional Requirements:

The general functional requirements of this equipment are to provide necessary control of the Standby Liquid Control System (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.

7.1.2.5 Information Systems Important to Safety

7.1.2.5.1 Post Accident Monitoring (PAM)

(1) Safety Design Bases

General Functional Requirements:

The general functional requirements of Post Accident Monitoring (PAM) are to provide the necessary display instrumentation in the MCR so the reactor operator can determine and accomplish the manual control actions required for safe plant operation during post accident events.

Specific Regulatory Requirements:

The specific regulatory requirements applicable to the PAM 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 MCR.

7.1.2.5.2 Process Radiation Monitoring System (PRM)

(1) Safety Design Bases

General Functional Requirements:

- (a) Monitor the gross radiation level in the main steam lines 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 MCR.
- (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 Safety System Logic and Control (SSL) to initiate 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 SGT 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 MCR can be maintained during an accident condition.

(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 MCR.
- (e) Provide alarm annunciation signals to the MCR 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 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.

7.1.2.5.3 Containment Monitoring System (CMS)

(1) Safety-related Design Bases

- (a) Monitor hydrogen, oxygen concentration, and gamma radiation levels in the drywell and wetwell air during normal plant operation and post accident conditions. Provide annunciation if radiation, hydrogen and oxygen alarm levels are reached or of a radiation, hydrogen and oxygen monitoring channel is in an inoperative state.
- (b) Monitor suppression pool (S/P) temperatures and upon exceeding a high limit, initiate suppression pool cooling mode of RHR and provide signals to the RPS for scram use. The suppression pool temperature monitoring (SPTM) function also isolates RBCW to the Reactor Water Cleanup System (RWCU) non-regenerative heat exchanger for heat load shedding to increase suppression pool cooling.

- (c) Provide drywell pressure signals for LOCA initiation, and for use by RPS for reactor scram, and for use by LDI for primary containment vessel (PCV) isolation.
 - (d) Lower drywell flooding (LDF) functions to flood the lower drywell with water from the suppression pool in the unlikely event of a severe accident where the core is postulated to melt and cause a subsequent vessel failure.
- (2) Non-Safety-Related Design Bases
- (a) Provide MCR display and alarms of the measured levels of PCV hydrogen, oxygen, radiation, temperature, dew point and pressure, and suppression pool temperature and level.
 - (b) Provide information to determine when the PCV is de-inerted and when personnel re-entry procedures may be initiated.
 - (c) Provide information to determine when the PCV is inerted and when nitrogen purging may be terminated.
 - (d) Obtain reactor water and other PCV atmosphere samples following an accident.
 - (e) Provide measurements, indication, and recording of suppression pool temperature during normal operation. Initiate alarms in the MCR and at the two remote shutdown panels when high temperature in the suppression pool is reached. The SPTM portion of CMS also provides temperature information on the Post-LOCA condition of the suppression pool.
 - (f) Provide measurements of the suppression pool water level.
 - (g) Perform the containment Integrated Leakage Rate Test (ILRT).

7.1.2.6 Interlock Systems Important to Safety

7.1.2.6.1 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.

7.1.2.6.2 Wetwell-to-Drywell Vacuum Breaker Interlocks

See Subsection 6.2.1.

7.1.2.7 Control Systems

(1) Safety Design Bases

The safety design basis for the Neutron Monitoring System is described in 7.1.2.7.1. All other control systems have no safety design bases. However, they are designed so that the functional capabilities of safety-related systems are not precluded.

Specific Regulatory Requirements

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

(2) Non-Safety-Related Design Basis

The non-safety-related design basis for each control system is discussed in Section 7.7.

7.1.2.7.1 Neutron Monitoring System (NMS)—Instrumentation and Controls

7.1.2.7.1.1 Startup Range Neutron Monitoring (SRNM) Subsystem

(1) Safety Design Bases

General Functional Requirements:

- (a) The Startup Range Neutron Monitoring (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 RPS (Section 7.1.2.2).

Specific Regulatory Requirements:

Specific regulatory requirements for the Neutron Monitoring System (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 (as specified in Section 7.7).
- (d) Provide a continuous measure of the time rate of change of neutron flux (reactor period) over the range from -100 seconds to $(-)$ infinity and $(+)$ infinity to $+10$ seconds.
- (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.

7.1.2.7.1.2 Local Power Range Monitor (LPRM) Subsystem

- (1) Safety Design Bases

General Functional Requirements:

The general functional requirement of the local power range monitor (LPRM) subsystem is to provide a sufficient number of LPRM signals to satisfy the average power range monitor (APRM) and oscillation power range monitor (OPRM) 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 reactor 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.

7.1.2.7.1.3 Average Power Range Monitor (APRM) Subsystem

- (1) Safety Design Bases

General Functional Requirements:

The general functional requirement is 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, and core flow rapid decrease trip. The independence and redundancy incorporated into the design of the APRM subsystem shall be consistent with the safety design bases of the RPS. The RPS design bases are discussed in Subsection 7.1.2.2.

The flow rate unit, as part of the APRM subsystem, converts the core plate differential pressure signal from the Main Steam System (MS) into a core flow signal. This flow signal provides the control and reference signal for the APRM and MBRM core flow-rate dependent trips.

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 (RCIR).

- (d) A simulated thermal power signal derived from each APRM channel which approximates the dynamic effects of the fuel.
- (e) A reference power level to permit trip in response to a reactor internal pump trip.

7.1.2.7.1.4 Oscillation Power Range Monitor (OPRM) Subsystem

- (1) Safety Design Bases

General Functional Requirement:

The design basis of the oscillation power range monitor (OPRM) is to provide a trip in order to prevent core flux oscillations from leading to a violation of core thermal limits. The OPRM does this while simultaneously discriminating against false signals from other parameter fluctuations that are not related to core instability.

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 OPRM shall provide the following functions:

- (a) 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.

7.1.2.7.1.5 Automated Traversing Incore Probe (ATIP) Subsystem

- (1) Safety Design Bases

None. The automated traversing probe (ATIP) subsystem portion of the NMS is non-safety-related.

- (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 either 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.

7.1.2.7.1.6 Multi-Channel Rod Block Monitor (MRBM) Subsystem

- (1) Safety Design Bases

None; the multi-channel rod block monitor (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.

7.1.2.8 Diverse Instrumentation and Control Systems

7.1.2.8.1 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 alternate rod insertion function (ARI) function are to:

- (a) Provide alternate and diverse method for inserting control rods using the ARI valves of the CRD (i.e., hydraulic insertion) or by using the FMCRD electric motors (i.e., electric motor insertion).
- (b) Provide for automatic and manual operation of this 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 FMCRD motors, shall be connected to a power bus that can automatically receive power from an emergency diesel generator, if necessary).
- (e) Mitigate the consequences of ATWS events.

7.1.2.9 Data Communication Systems

7.1.2.9.1 Multiplexing System

(1) Safety Design Bases

The Essential Multiplexing System (EMS) portion of MUX has the following safety design basis:

EMS acquires process measurements and equipment status data, conditions and formats the data and then transmits the data to the MCR area. The data processed for each plant safety system in the Safety System Logic and Control system (SSLC) and other Class 1E controllers are then transmitted, via EMS, to distribution points where the signals are hardwired for use by device drivers (e.g., motor control centers (MCCs), switchgear, etc.).

The Non-Essential Multiplexing System (NEMS) portion of MUX has no safety related functions.

(2) Non-Safety-Related Design Bases

The MUX shall meet the following power generation design bases:

- (a) EMS transmits alarm and status from safety-related plant sensors and SSLC to the non-safety-related plant-wide NEMS for MCR indication and computer logging through an isolated gateway interface.
- (b) EMS transmits selected sensed safety-related plant data to the non-safety-related transient analysis and recording sub-system of Plant Computer System (PCS) through an isolated gateway interface.
- (c) EMS transmits selected safety-related plant data to the non-safety-related control systems through an isolated gateway interface.
- (d) EMS provides data message formatting and transmission of the data from the remote locations to the MCR via fiber optic networks.
- (e) NEMS acquires process measurement and equipment status signals from the process sensors and discrete monitors of the plant's systems.
- (f) NEMS performs signal conditioning and analog-to-digital (A/D) conversion for the continuous process signals. NEMS performs signal conditioning and change-of-state detection for the discrete signals.
- (g) NEMS provides data message formatting and transmission of the data from the remote location to the MCR via fiber optic networks.

- (h) NEMS transmits the acquired data to the Control and Display Interface, a subset of the Plant Computer System.
- (i) NEMS receives the command and control signals from the intelligent (dual and triply redundant) controllers in the MCR area, and transmits the signals from the MCR area to the remote locations where NEMS distributes the signals to the final actuating devices.
- (j) NEMS provides data support functions [e.g., Technical Support Center (TSC), Emergency Operations Facility (EOF)] and operator aids.

7.1.2.10 Conformance to Regulatory Requirements

7.1.2.10.1 Regulation 10CFR50.55a and 10CFR50.34 (f)(2)

Table 7.1-2 identifies the application of various criteria to all I&C systems. They are also discussed in the analysis portions of Sections 7.2 through 7.9.

7.1.2.10.2 Regulation 10CFR50 Appendix A

Conformance with NRC General Design Criteria (GDC) 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 7.9. Individual systems application to GDCs identified in the Standard Review Plan for Chapter 7 are shown on Table 7.1-2.

7.1.2.11 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 7.9. SSLC, as the supporting physical and functional structure of the safety-related systems, complies with these guides to the same extent as the supporting systems.

7.1.2.11.1 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 HICB-8) are discussed in the analysis portions of Sections 7.2 through 7.9.

7.1.2.11.2 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, and Regulatory Guide 1.47. Additional information may be found in the system detail descriptions

in Sections 7.2 through 7.9. 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 effects 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.

7.1.2.11.3 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 through 7.9 provide further discussion.

7.1.2.11.4 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. The applicable system descriptions or analysis portions of Sections 7.2 through 7.6, and 7.8.

7.1.2.11.5 Regulatory Guide 1.75—Physical Independence of Electric Systems

The safety-related systems described in Sections 7.2 through 7.9 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.

7.1.2.11.6 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.

7.1.2.11.7 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.

7.1.2.11.8 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.

7.1.2.11.9 Regulatory Guide 1.105—Instrument Setpoints

The I&C systems will be consistent with the requirements of Regulatory Guide 1.105. The trip setpoint (instrument setpoint), allowable value (Tech Spec limit) and the analytical or design basis limit are all contained in the Technical Specifications (Chapter 16) for the FSAR. These parameters will be appropriately separated from each other based on instrument accuracy, calibration capability and design drift (estimated) allowance data. The setpoints will be within the instrument best accuracy range. The established setpoints will provide margin to satisfy both safety requirements and plant availability objectives.

7.1.2.11.10 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 Section 7.2.

7.1.2.11.11 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.

7.1.2.11.12 Regulatory Guide 1.152 - Digital Computers in Safety Systems

This Regulatory Guide is applicable to the SSLC, and its supported I&C systems, and also to all other safety-related software-based controllers. Such controllers are consistent with this guide, as delineated in Section 7.2 and 7.3. Hardware and Software are integrated into a final assembly that is validated by testing against input requirements.

7.1.2.11.13 Regulatory Guide 1.153 - Power Instrumentation & Control Portions of Safety Systems

Instrumentation and controls are designed to meet the requirements of Regulatory Guide 1.153, as discussed in the analysis portions of Section 7.2 through 7.6 and 7.9.

7.1.2.11.14 Draft Regulatory Guide DG-1054 - Verification, Validation, Reviews, And Audits For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants.

This regulatory guide endorses IEEE Std 1012, IEEE Standard for Software Verification and Validation Plans, and IEEE Std 1028, IEEE Standard for Software Reviews and Audits. IEEE Std 1012 is acceptable for providing high functional reliability and design quality in software used in safety systems IEEE Std 1028 is acceptable for carrying out software reviews, inspections, walkthroughs, and audits subject to certain provisions. SSLC software development uses the guidance in these standards as discussed in Section 7.1.1.2.1.3(b) to develop portions of the overall software development plan and thus fully complies with this Reg Guide.

7.1.2.11.15 Draft Regulatory Guide DG-1055 - Configuration Management Plans For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants

This regulatory guide endorses IEEE Std 828, IEEE Standard for Software Configuration Management Plans, and ANSI/IEEE Std 1042, IEEE Guide to Software Configuration Management. These standards, with the clarifications provided in the Regulatory Position, describe acceptable methods for providing high functional reliability and design quality in software used in safety systems. SSLC software development uses the guidance in these

standards as discussed in Section 7.1.1.2.1.3(b) to develop portions of the overall software development plan and thus fully complies with this Reg Guide.

7.1.2.11.16 Draft Regulatory Guide -1056 - Software Test Documentation For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants

The requirement contained in IEEE Std 829, IEEE Standard for Software Test Documentation, provide an acceptable approach for meeting the requirements of 10 CFR Part 50 as they apply to the test documentation of safety system software subject to the provisions in this guide. SSLC software development uses the guidance in these standards as discussed in Section 7.1.1.2.1.3(b) to develop portions of the overall software development plan and thus fully complies with this Reg Guide.

7.1.2.11.17 Draft Regulatory Guide DG-1057 - Software Unit Testing For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants

This regulatory guide endorses IEEE Std 1008, IEEE Standard for Software Unit Testing, subject to the provisions in this guide. This standard defines an acceptable method for planning, preparing for, conducting, and evaluating software unit testing. SSLC software development uses the guidance in this standard as discussed in Section 7.1.1.2.1.3(b) to develop portions of the overall software development plan and thus fully complies with this Reg Guide.

7.1.2.11.18 Draft Regulatory Guide DG-1058 - Software Requirements Specifications For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants

This regulatory guide endorses IEEE Std 830, Recommended Practice for Software Requirements Specifications, as amended in the Regulatory Position. This standard describes current practice for writing software requirements specifications for a wide variety of systems. It is not specifically aimed at safety applications; however, it does provide guidance on the development of software requirements specifications that will exhibit characteristics important for developing safety system software. This is consistent with the goal of ensuring high-integrity software in reactor safety systems. SSLC software development uses the guidance in this standard as discussed in Section 7.1.1.2.1.3(b) to develop portions of the overall software development plan and thus fully complies with this Reg Guide.

7.1.2.11.19 Draft Regulatory Guide DG-1059 - Developing Software Life Cycle Processes For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants

This regulatory guide endorses IEEE Std 1074. The standard describes, in terms of inputs, development, verification or control processes, and outputs, a set of processes and constituent activities that are commonly accepted as composing a controlled and well-coordinated software-development process. It describes inter-relationships among activities by defining the source activities that produce the inputs and the destination activities that receive the outputs. The standard specifies activities that must be performed and their inter-relationships; it does not specify complete acceptance criteria for determining whether the activities themselves are

properly designed. Therefore, the standard should be used in conjunction with guidance from other appropriate regulatory guides, standards, and software engineering literature. SSLC software development uses the guidance in this standard as discussed in Section 7.1.1.2.1.3(b) to develop portions of the overall software development plan and thus fully complies with this Reg Guide.

7.1.2.12 Conformance to Industry Standards

7.1.2.12.1 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 through 7.9.

7.1.2.12.2 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).

7.1.2.12.3 IEEE 338—Standard Criteria for Periodic Testing of Nuclear Power Generating Station Class 1E 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 through 7.9.

7.1.2.12.4 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.

7.1.2.12.5 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 through 7.9.

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

The safety-related systems described in Sections 7.2 through 7.9 meet the independence and separation criteria for redundant systems in accordance with IEEE 384. See Subsection 7.1.2.11.5 for conformance to Regulatory Guide 1.75.

7.1.2.12.7 IEEE 603—Standard Criteria for Safety Systems for Nuclear Power Generating Stations

IEEE-603 extends IEEE-279 to include ESF in addition to RPS. The safety-related Systems described in Sections 7.2 through 7.9 and the supporting SSLC equipment described in Subsection 7.1.1.2.1 meet all criteria in IEEE-603.

7.1.2.13 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 7.9. Conformance of SSLC to the BTPs related directly to the development and operation of SSLC microprocessor-controlled equipment are discussed below:

- (1) BTP-HICB-11: Guidance on Application and Qualification of Isolation Devices

SSLC logic controllers use fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections from safety-related to non-safety-related devices.

Certain diverse and hardwired portions of RPS may use coil-to-contact isolation of relays or contactors. This is acceptable according to the BTP when the application is analyzed or tested per the guidelines of Reg Guide 1.75 and Reg Guide 1.153.

- (2) BTP-HICB-14: Guidance on Software Reviews for Digital Computer-based Instrumentation and Control Safety Systems

Development of software for the safety system functions within SSLC conforms to the guidance of this BTP as discussed in Section 7.1.1.2.1.3(b). Safety-related software to be embedded in the memory of the SSLC controllers is developed according to a structured plan (MMIS Design Implementation Plan) comprising a Software Management Plan, Software Configuration Management Plan, and Software Verification and Validation Plan. These plans follow the software life cycle process described in the BTP.

- (3) BTP-HICB-17: Guidance on Self-Test and Surveillance Test Provisions in Digital Computer-based Instrumentation and Control Systems

The SSLC controllers conform to this BTP as discussed in Section 7.1.2.1.6.

- (4) BTP-HICB-18: Guidance on Use of Programmable Logic Controllers in Digital Computer-based Instrumentation and Control Systems

Portions of SSLC design that use commercial grade PLCs for safety-related functions conform to this BTP (and to BTPs 14, 17, and 21) in that the PLCs will be qualified to a level commensurate with safety system requirements.

- (5) BTP-HICB-19: Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems

SSLC is a 4-division, independent and separated equipment arrangement. Isolation of signal transmission between safety-related divisions and between safety-related and non-safety-related equipment employs non-conductive fiber-optic cable. System functions are segmented among multiple controllers. Automatic functions are backed up by diverse manual functions. Control system functions are separate, independent, and diverse from the protection system. Additional diverse features are included as discussed in Section 7.8.

- (6) BTP-HICB-21: Guidance on Evaluation of Digital System Architecture and Real-Time Performance

The real-time performance of SSLC in meeting the requirements for safety system trip and initiation response conforms to this BTP. Each SSLC controller operates independently and asynchronously with respect to other controllers so that timing can readily be evaluated from input to output of each controller. Timing signals are not exchanged between divisions of independent equipment or between controllers within a division.

7.1.2.14 Conformance to TMI Action Plan Requirements

TMI action plan requirements are contained in 10CFR50.34 (f), and are generically addressed in Appendix 1A. Those applicable to I&C are identified in Table 7.1-2 as 10CFR50.34(f)(2). Clarifications or exceptions related specifically to I&C (if any) are addressed in the analysis portions of Sections 7.2 through 7.9.

7.1.2.15 Additional Design Consideration Analyses

7.1.2.15.1 Cooling Temperature Profiles for Class 1E Digital Equipment

Cooling temperature profiles for cabinets containing Class 1E microprocessor-based equipment will be addressed in the FSAR. The profiles shall include data for HVAC configurations consistent with the various accident events which require engineered safety features (ESF) systems.

7.1.2.15.2 Electrostatic Discharge on Exposed Equipment Components

EPRI TR-102323, Guidelines for Electromagnetic Interference in Power Plants, does not consider electrostatic discharge (ESD) as a common-mode failure mechanism for safety-related digital systems because ESD is a localized effect. However, it is recognized as a failure mechanism for digital components and is a prudent test to be performed in developing digital control systems. Therefore, the effects of ESD at keyboards, keyed switches, and other exposed equipment must be limited. Various grounding, shielding, and circuit design techniques will be employed, with the standards specified in Section 7.2.1.1.7(5) being used for guidance. EPRI TR-102323 provides recommendations for test methods. The FSAR will describe the ESD control program that will be established during design and development of the actual plant I&C equipment.

7.1.2.15.3 Localized High Heat Spots in Semiconductor Materials for Computing Devices

High current densities in modern high-speed semiconductors and complex integrated circuits may result in localized hot spots in semiconductor materials used in computing devices. The FSAR will describe the method of equipment specification that will minimize the effects of hot spots. The FSAR will also address thermal analyses that are required to be performed at the circuit board, instrument, and panel design stages.

Table 7.1-1 System Coverage within Safety System Logic and Control (SSLC) *

System Logic residing in SSLC (C74) Controllers	Product Structure		SSLC Output Response Per System	
	Sys ID	Sys Code	Actuator Response to Trip Output on Demand for Trip	Output Response to Power or Signal Loss
A. Reactor Protection System (reactor trip)	RPS	C71	De-energize	Fail-safe (trip)
B. Main Steam System (non-ADS SRV)	MS	B21	Energize	Fail-as-is (no change)
C. Engineered Safety Features (ESF)				
1. Emergency Core Cooling Systems (ECCS)				
a. Reactor Core Isolation Cooling	RCIC	E51	Energize	Fail-as-is
b. Residual Heat Removal/LPFL mode	RHR	E11	Energize	Fail-as-is
c. High Pressure Core Flooder	HPCF	E22	Energize	Fail-as-is
d. Automatic Depressurization System (ADS)		(B21)	Energize	Fail-as-is
2. Leak Detection and Isolation System	LDI	C73		
a. Main Steam Isolation Valves (MSIV)		(B21)	De-energize	Fail-safe
b. PCV Isolation				
i. RCIC		(E51)	De-energize	Fail-safe
ii. RHR		(E11)	De-energize	Fail-safe
iii. Reactor Water Cleanup (RWCU)		(G31)	De-energize	Fail-safe
iv. Other PCV Isolation Valves (part of auxiliary ESF systems below)			De-energize	Fail-safe
3. Auxiliary ESF Systems				
a. Reactor Building Cooling Water	RBCW	P21	Energize	Fail-as-is
b. Emergency Chilled Water	ECW	P25	Energize	Fail-as-is
c. Reactor Building Service Water	RBSW	P26	Energize	Fail-as-is

Table 7.1-1 System Coverage within Safety System Logic and Control (SSLC) (Continued)*

System Logic residing in SSLC (C74) Controllers	Product Structure		SSLC Output Response Per System	
	Sys ID	Sys Code	Actuator Response to Trip Output on Demand for Trip	Output Response to Power or Signal Loss
d. Nitrogen Supply System [†]	N2	P54	Energize	Fail-as-is
e. Electrical Power Distribution	EPD	R10	Energize	Fail-as-is
f. Emergency Diesel Generator	DG	R21	Energize	Fail-as-is
g. Standby Gas Treatment System	SGT	T22	Energize	Fail-as-is
h. Atmospheric Control System [†]	ACS	T31	Energize	Fail-as-is
i. Reactor Building HVAC	RBHV	T41	Energize	Fail-as-is
j. Control Building HVAC	CBHV	T43	Energize	Fail-as-is
k. Containment Monitoring System - Suppression Pool Temperature Monitoring (SPTM) function	CMS	T62	Energize	Fail-as-is
l. Ultimate Heat Sink	UHS	W11	Energize	Fail-as-is

* The safety control and interlock functions (automatic and manual) of the following systems are performed by software within the microprocessor-based control equipment of SSLC (some manual control functions may be implemented external to microprocessor logic).

† These systems have PCV isolation valves controlled by LDI.

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

Applicable Criteria	10CFR								10CFR50, App. A, General Design Criteria											
	50.55a	50.34 (f) (2) (v) (I.D.3)	50.34 (f) (2) (xvii) II.F.1)	50.34 (f) (2) (xviii) (II.F.2)	50.34 (f) (2) (xiv) (II.E.4.2)	50.34 (f) (2) (xix) (II.F.3)	50.34 (f) (2) (xxiv) (II.K.3.23)	50.62	1	2	4	13	19	20	21	22	23	24	25	29
Reference Standard	IEEE 279	NUREG 718, 737, 694	NUREG 718, 737, 694	NUREG 694	NUREG 737	NUREG 718	NUREG 718													
Reactor Protection System	X	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
Leak Detection & Isolation	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		X
RHR/Supp. Pool Cooling	X	X			X				X	X	X	X	X	X	X	X	X	X		X
Standby Gas Treatment	X	X			X				X	X	X	X	X	X	X	X	X	X		X
Emergency Diesel Support Systems	X	X							X	X	X	X	X							
Reactor Bldg. Cooling and Service Water	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	X		X
Emergency Chilled Water System	X	X							X	X	X	X	X	X	X	X	X	X		X
Nitrogen Supply System	X	X			X				X	X	X	X	X	X	X	X	X	X		X
Flammability Control System	X	X							X	X	X	X	X	X	X	X	X	X		X
RHR/Shutdown Cooling	X								X	X	X	X	X					X		
Remote Shutdown System	X								X	X	X	X	X					X		
Standby Liquid Control	X								X	X	X	X	X					X		
Post Accident Monitoring		X	X	X		X	X		X	X	X	X	X							
Process Radiation Monitoring	X	X	X			X			X	X	X	X	X	X	X	X	X	X		
Containment Monitoring System	X	X	X			X			X	X	X	X	X					X		
Interlock Systems Important to Safety	X	X							X	X	X	X	X					X		
Main Steam System									X			X	X					X		
Rod Control and Information System									X			X	X					X		
Recirculation Flow Control System									X			X	X					X		
Feedwater Control System									X			X	X					X		
Process Computer System									X			X	X					X		
Neutron Monitoring System	X								X	X	X	X	X	X	X	X	X	X	X	X
Automatic Power Regulator System									X			X	X					X		
Steam Bypass and Pressure Control System									X			X	X					X		
Fuel Pool Cooling and Cleanup Systems									X			X	X					X		
Diverse Instrumentation and Control	X							X	X									X		
Data Communications Systems	X	X						X	X	X	X	X	X		X	X	X	X		X

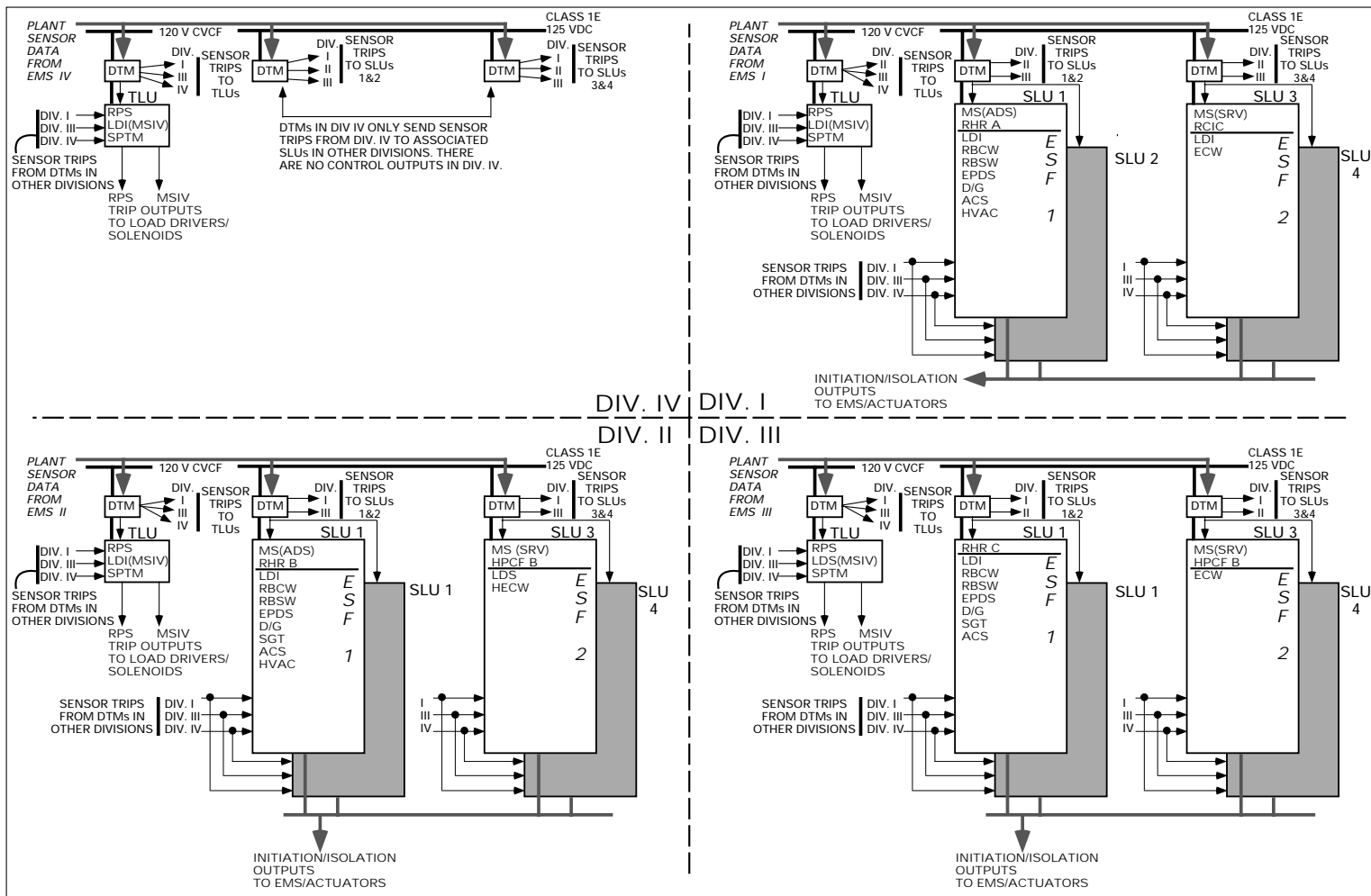
Table 7.1-2 Regulatory Requirements Applicability Matrix for I&C Systems (Continued)

Applicable Criteria	Regulatory Guides														Branch Technical Positions (BTP)																	
	1.22	1.47	1.53	1.62	1.75	1.97	1.105	1.118	1.151	1.152*	1.153	Draft Reg. Guide DG-1055*	Draft Reg. Guide DG-1054*	Draft Reg. Guide DG-1058*	Draft Reg. Guide DG-1056*	Draft Reg. Guide DG-1057*	Draft Reg. Guide DG-1059*	HICB-1	HICB-3	HICB-6	HICB-8	HICB-9	HICB-10	HICB-11	HICB-12	HICB-14*	HICB-17*	HICB-18*	HICB-19*	HICB-21*		
Reference Standard	IEEE 279		IEEE 379	IEEE 279	IEEE 384	ANSI/ANS 4.5	ISA S67.04	IEEE 338	ISA S67.02	IEEE 7-4.3.2	IEEE 603	IEEE 828, 1042	ANSI/IEEE 1012, 1028	IEEE 830	ANSI/IEEE 829	ANSI/IEEE 1008	IEEE 1074	GDC 15	IEEE 279, 603	IEEE 279, 603	R.G. 1.22	R.G. 1.153	R.G. 1.97	R.G. 1.75, 1.153	R.G. 1.105	NUREG/CR-6101	IEEE 279, 603	NUREG/CR-6090	NUREG/CR-6303	NUREG/CR-6083		
Reactor Protection System	X	X	X	X	X		X	X		X	X	X	X	X	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		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			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	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	X	X					X			X	X	X	X	X	X	X	X
Standby Gas Treatment	X	X	X	X	X		X	X		X	X	X	X	X	X	X	X					X			X	X	X	X	X	X	X	X
Emergency Diesel Support Systems	X	X	X	X	X		X	X		X	X	X	X	X	X	X	X					X			X	X	X	X	X	X	X	X
Reactor Bldg. Cooling and Service Water	X	X	X	X	X		X	X		X	X	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	X	X	X	X					X			X	X	X	X	X	X	X	X
Emergency Chilled Water Systems	X	X	X	X	X		X	X		X		X	X	X	X	X	X					X			X	X	X	X	X	X	X	X
Nitrogen Supply System	X	X	X	X	X		X	X		X	X	X	X	X	X	X	X					X			X	X	X	X	X	X	X	X
Flammability Control System	X	X	X	X	X		X	X		X	X											X			X	X						
RHR/Shutdown Cooling	X	X	X	X	X		X	X		X	X	X	X	X	X	X	X								X	X	X	X	X	X		X
Remote Shutdown System			X	X	X						X																					
Standby Liquid Control	X	X	X	X	X		X	X		X	X												X			X	X	X				
Post Accident Monitoring						X																		X								
Process Radiation Monitoring	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X					X			X	X	X	X	X	X		X
Containment Monitoring System	X	X	X		X	X	X	X		X	X	X	X	X	X	X	X							X	X	X	X	X	X	X		X
Interlock Systems Important to Safety	X	X	X	X	X		X	X		X	X	X	X	X	X	X	X	X	X						X	X	X	X	X	X		X
Main Steam System									X																							
Neutron Monitoring System	X	X	X		X	X	X	X		X	X	X	X	X	X	X	X					X		X	X	X	X	X	X	X	X	X
Diverse Instrumentation and Control	X			X	X		X	X		X		X	X	X	X	X	X								X	X	X	X	X	X	X	X
Data Communications Systems	X	X	X		X		X	X		X	X	X	X	X	X	X	X					X			X	X	X	X	X	X	X	X

* These criteria are addressed in conjunction with the Safety System Logic and Control System (SSLC) which is the logic and control interface with the identified systems. See Subsections 7.1.2.11 through 7.1.2.13.

Table 7.1-3 I&C Systems for which Logic Diagrams will be Provided in the FSAR

Safety System Logic and Control (SSLC)
Reactor Protection System (RPS)
High Pressure Core Flooder System (HPCF)
Main Steam System (MS)
Reactor Core Isolation Cooling System (RCIC)
Residual Heat Removal System (RHR)
Leak Detection and Isolation System (LDI)
Standby Gas Treatment System (SGT)
Reactor Building Cooling Water System (RBCW)
Reactor Building Service Water System (RBSW)
Control Building HVAC (CBHV)
Reactor Building HVAC (RBHV)
Auxiliary Fuel Building HVAC (AFHV)
Emergency Chilled Water System (ECW)
Nitrogen Supply System (N ₂)
Flammability Control System (FCS)
Remote Shutdown System (RSD)
Standby Liquid Control System (SLC)
Process Radiation Monitoring System (PRM)
Containment Monitoring System (CMS)
Rod Control and Information System (RCIS)
Recirculation Flow Control System (RFC)
Feedwater Control System (FWC)
Plant Computer System (PCS)
Neutron Monitoring System (NMS)
Automatic Power Regulator System (APR)
Steam Bypass and Pressure Control System (SBPC)
Fuel Pool Cooling and Cleanup System (FPCU)
Auxiliary Fuel Pool Cooling and Cleanup System (FPCU)
Multiplexing System (MUX)



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

ACS = ATMOSPHERIC CONTROL
 DG = DIESEL GENERATOR
 EPDS = ELECTRICAL POWER DISTRIBUTION SYSTEM
 ESF = ENGINEERED SAFETY FEATURES
 ECW = HVAC EMERGENCY COOLING WATER
 HVAC = HEATING, VENTILATING & AIR CONDITIONING
 LDI = LEAK DETECTION & ISOLATION SYSTEM
 MSIV = MAIN STEAM ISOLATION VALVE
 MS = MAIN STEAM SYSTEM

NMS = NEUTRON MONITORING SYSTEM
 PRM = PROCESS RADIATION MONITORING
 RCIC = REACTOR CORE ISOLATION COOLING
 RBCW = REACTOR BUILDING CLOSED COOLING WATER
 RHR = RESIDUAL HEAT REMOVAL
 RPS = REACTOR PROTECTION SYSTEM
 RBSW = REACTOR SERVICE WATER
 SGT = STANDBY GAS TREATMENT SYSTEM
 SPTM = SUPPRESSION POOL TEMPERATURE MONITORING

NOTES:
 1. NMS AND PRM (NOT SHOWN) ARE STAND ALONE 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/PRM: CLASS 1E, 120 V CVCF

Figure 7.1-1 Assignment of Interfacing Safety System Logic to SSLC Controllers